561 COMPLETED Y4.J89/1:99/50

# ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

M-219

# HEARINGS

BEFORE THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

FIRST AND SECOND SESSIONS

ON

H.R. 3378

ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

SEPTEMBER 26, OCTOBER 24, 1985, JANUARY 30, AND MARCH 5, 1986

---

**Serial No. 50**

ORIGINAL

N/CAD

# ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

# HEARINGS

BEFORE THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

FIRST AND SECOND SESSIONS

ON

## H.R. 3378

ELECTRONIC COMMUNICATIONS PRIVACY ACT

SEPTEMBER 26, OCTOBER 24, 1985, JANUARY 30, AND MARCH 5, 1986

**Serial No. 50**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
58-844 O WASHINGTON : 1986

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

## COMMITTEE ON THE JUDICIARY

PETER W. RODINO, Jr., New Jersey, *Chairman*

JACK BROOKS, Texas
ROBERT W. KASTENMEIER, Wisconsin
DON EDWARDS, California
JOHN CONYERS, Jr., Michigan
JOHN F. SEIBERLING, Ohio
ROMANO L. MAZZOLI, Kentucky
WILLIAM J. HUGHES, New Jersey
MIKE SYNAR, Oklahoma
PATRICIA SCHROEDER, Colorado
DAN GLICKMAN, Kansas
BARNEY FRANK, Massachusetts
GEO. W. CROCKETT, Jr., Michigan
CHARLES E. SCHUMER, New York
BRUCE A. MORRISON, Connecticut
EDWARD F. FEIGHAN, Ohio
LAWRENCE J. SMITH, Florida
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
HARLEY O. STAGGERS, Jr., West Virginia
JOHN BRYANT, Texas

HAMILTON FISH, Jr., New York
CARLOS J. MOORHEAD, California
HENRY J. HYDE, Illinois
THOMAS N. KINDNESS, Ohio
DAN LUNGREN, California
F. JAMES SENSENBRENNER, Jr., Wisconsin
BILL McCOLLUM, Florida
E. CLAY SHAW, Jr., Florida
GEORGE W. GEKAS, Pennsylvania
MICHAEL DEWINE, Ohio
WILLIAM E. DANNEMEYER, California
HANK BROWN, Colorado
PATRICK L. SWINDALL, Georgia
HOWARD COBLE, North Carolina

M. Elaine Mielke, *General Counsel*
Garner J. Cline, *Staff Director*
Alan F. Coffey, Jr., *Associate Counsel*

---

## Subcommittee on Courts, Civil Liberties, and the Administration of Justice

ROBERT W. KASTENMEIER, Wisconsin, *Chairman*

JACK BROOKS, Texas
ROMANO L. MAZZOLI, Kentucky
MIKE SYNAR, Oklahoma
PATRICIA SCHROEDER, Colorado
BARNEY FRANK, Massachusetts
BRUCE A. MORRISON, Connecticut
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia

CARLOS J. MOORHEAD, California
HENRY J. HYDE, Illinois
MICHAEL DEWINE, Ohio
THOMAS N. KINDNESS, Ohio
PATRICK L. SWINDALL, Georgia
HOWARD COBLE, North Carolina

Michael J. Remington, *Chief Counsel*
Gail Higgins Fogarty, *Counsel*
David W. Beier, *Counsel*
Deborah Leavy, *Counsel*
Thomas E. Mooney, *Associate Counsel*
Joseph V. Wolfe, *Associate Counsel*

# CONTENTS

## HEARINGS HELD

Page

September 26, 1985 .......... 1

October 24, 1985 .......... 41

January 30, 1986 .......... 107

March 5, 1986 .......... 211

## WITNESSES

Amick, Neal J., division manager, AT&T .......... 108

Prepared statement .......... 111

Cavanagh, Michael F., executive director, Electronic Mail Association .......... 18

Colgan, Richard T., executive secretary, Association of North American Radio Clubs .......... 147

Prepared statement .......... 171

Fishman, Clifford S., professor of law, Catholic University of America Law School .......... 254

Prepared statement .......... 258

Hess, Frederick D., director, Office of Enforcement Operations, Department of Justice .......... 212

Knapp James, deputy assistant attorney general, Department of Justice .......... 212

Prepared statement .......... 218

Kelly, John W., Jr., attorney, Southwestern Bell Telephone Co .......... 108

Prepared statement .......... 135

Kuhnreich, George A., vice president, Tandy Corp .......... 147

Prepared statement .......... 157

Leahy, Hon. Patrick J., U.S. Senator from the State of Vermont .......... 3

Prepared statement .......... 5

Nugent, P. Michael, chairman, Committee on Computer Systems and Communications Privacy, ADAPSO .......... 74

Prepared statement .......... 77

Quigley, Philip J., president and chief executive officer, pacTel Mobile Co.'s .......... 26

Prepared statement .......... 29

Stanton, John W., chairman, Telocator Network of America .......... 92

Prepared statement .......... 95

Walker, Philip M., general regulatory counsel, GTE Telenet Inc .......... 18

Weingarten, Fred W., program manager, Communication and Technologies Program, Office of Technology Assessment .......... 42

Prepared statement .......... 46

Williams, Perry F., secretary, the American Radio Relay League, Inc .......... 147

Prepared statement .......... 148

## ADDITIONAL MATERIAL

Article from the New York Post, "E-Mail Bill Focuses on Security," dated September 10, 1985 .......... 9

Article from the New York Times, "New Law to Protect Computer Data Sought," dated September 19, 1985 .......... 10

Letter to Hon. William French Smith, Attorney General of the United States from Patrick Leahy, U.S. Senator, dated January 26, 1984 with enclosures ... 11

## APPENDIX

Page

Letter from John R. Bolton, Assistant Attorney General, U.S. Department of Justice to Hon. Peter W. Rodino (June 6, 1986) ........ 279

Letter from Edward W. Hummers, Jr. to Hon. Robert W. Kastenmeier (May 12, 1986) ........ 280

Letter from Jerry W. Cox, Counsel for Dynascan Corporation to Hon. Robert W. Kastenmeier (April 29, 1986) ........ 282

Letter from Alexander B. Trowbridge, President, National Association of Manufacturers to Hon. Edwin Meese (April 29, 1986) ........ 286

Letter from R.S. Willis, Vice President, Associated Credit Services, Inc. to Subcommittee on Courts Civil Liberties and the Administration of Justice (April 25, 1986) ........ 288

Letter from John R. Bolton, Assistant Attorney General, U.S. Department of Justice to Hon. Robert W. Kastenmeier (April 15, 1986) ........ 289

Letter from Ward H. White, Vice President, United States Telephone Association to Hon. Robert W. Kastenmeier (April 14, 1986) ........ 292

Letter from Michelle Meier, Consumers Union to Hon. Robert W. Kastenmeier (April 9, 1986) ........ 294

Letter from Ted A. Heydinger, Vice President, Government Relations, CBEMA to Hon. Robert W. Kastenmeier (April 9, 1986) ........ 296

Letter from John W. Roach, President, Tandy Corporation to Hon. Robert W. Kastenmeier (April 9, 1986) ........ 293

Letter from Travis Marshall, Senior Vice President, Motorola, Inc. to Hon. Robert W. Kastenmeier (April 8, 1986) ........ 298

Letter from L. Ralph Mecham, Director, Administrative Office of the United States Courts to Hon. Peter W. Rodino (March 25, 1986) ........ 301

Letter from John Spain, President, Radio-Television News Directors Association to Hon. Robert W. Kastenmeier (March 18, 1986) ........ 302

Letter from F.W. Gerbracht, Jr., Vice President, Chase Manhattan Bank to Hon. Robert W. Kastenmeier (March 17, 1986) ........ 305

Letter from Jerry J. Berman, Chief Legislative Counsel, ACLU to Hon. Robert W. Kastenmeier (March 14, 1986) ........ 307

Letter from William H. Dempsey, Presdent, Association of American Railroads to Hon. Robert W. Kastenmeier (March 14, 1986) ........ 309

Statement of Edward O. Fritts, Presdent, National Association of Broadcasters before the Subcommittee on Courts, Civil Liberties and the Administration of Justice (March 7, 1986) ........ 312

Supplemental Statement of ANARC concerning H.R. 3378 "The Electronic Communications Privacy Act of 1985" (February 27, 1986) ........ 323

Letter from Hon. Robert W. Kastenmeier to Hon. Edwin Meese III, Attorney General of the United States Department of Justice (February 19, 1986) ........ 359

Letter from Robert A. McConnell, Vice President, CBS Washington, to Hon. Robert W. Kastenmeier (February 4, 1986) ........ 363

Testimony of Richard L. Brown before the Subcommittee on Courts, Civil Liberties and the Administration of Justice on behalf of Regency Electronics. Inc. (January 30, 1986) ........ 373

Statement of Richard L. Brown before the Subcommittee on Courts, Civil Liberties and the Administration of Justice on behalf of SPACE (January 30, 1986) ........ 392

Letter from Richard L. Brown to Hon. Robert W. Kastenmeier (January 28, 1986) ........ 396

Letter from Michael Goldsmith, Associate Professor of Law, Brigham Young University to Hon. Robert W. Kastenmeier (January 10, 1986) ........ 400

Letter from Bruce J. Eggers, Director, Congressional Relations, Ameritech to Hon. Robert W. Kastenmeier (December 17, 1985) ........ 405

Letter from Richard L. Brown, Counsel to the Satellite Television Industry Association/SPACE to Hon. Robert W. Kastenmeier (December 3, 1985) ........ 407

Letter from Leslie C. Seeman, General Counsel, The Source Information Network to Hon. Robert W. Kastenmeier (November 21, 1985) ........ 409

Letter from Christy E. Massie, Counsel, Administration Office of the United States Court to James C. Murr, Office of Management and Budget (October 31, 1985) ........ 413

Memo from James S. Golden, Southwestern Bell Corporation to Subcommittee on Courts, Civil Liberties and the Administration of Justice (October 31, 1985) ........ 415

| | Page |
|---|---|
| Letter from Hubert F. Owens, General Attorney, Bell South Corporation to the Subcommittee on Courts, Civil Liberties and the Administration of Justice (October 22, 1985) | 425 |
| Letter from Douglass J. McCollum, Attorney, C&P Telephone to the Subcommittee on Courts, Civil Liberties and the Administration of Justice (October 22, 1985) | 428 |
| Letter from Warren G. Austin, General Attorney, Northwestern Bell to the Judiciary Committee (September 30, 1985) | 430 |
| Memo from Jerry J. Berman and Marc Rotenberg, ACLU, to Conferees and Interested Persons (September, 1984) | 432 |
| Letter from Martin T. McCue, Director of Government Relations, Centel Corporation to Hon. Robert W. Kastenmeier (July 17, 1985) | 450 |
| Letter from Jerry J. Berman, Legislative Counsel, ACLU to Hon. Robert W. Kastenmeier (June 26, 1985) | 464 |
| Memo from ACLU Project Staff to Conferees and Interested Persons (June, 1985) | 469 |
| Letter from Lynn W. Ellis, Chairman, IEEE to Hon. Robert W. Kastenmeier (May 24, 1985) | 481 |
| Letter from Mary C. Lawton, Counsel for Intelligence Policy, U.S. Department of Justice (May 20, 1985) | 484 |
| Statement of Uniden Corporation of America before the House Subcommittee on Courts, Civil Liberties and the Administration of Justice | 501 |
| Statement of Pacific Telesis Group for Recommendations for Amendments | 517 |
| Statement of the National Association of Business & Educational Radio Concerning the "Electronic Communications Privacy Act of 1985" | 519 |
| Analysis of H.R 3378 (Same as S. 1667) "Electronic Communications Privacy Act of 1985" by AT&T | 523 |
| Comments of H.W. William Caming, Attorney and Consultant, upon "Electronic Communications Privacy Act of 1985" | 546 |

# ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

THURSDAY, SEPTEMBER 26, 1985

House of Representatives,
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice,
Committee on the Judiciary,
*Washington, DC.*

The subcommittee met, pursuant to call, at 10 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier and Moorhead.

Staff present: Deborah Leavy and David W. Beier, assistant counsel; Joseph V. Wolfe, associate counsel; and Audrey K. Marcus, clerk.

Mr. **Kastenmeier**. The committee will come to order.

This morning we begin a series of hearings on H.R. 3378, the Electronic Communications Privacy Act of 1985. This bill is the product of more than 2 years of work by this subcommittee, and, I am happy to say, enjoys the cosponsorship of the ranking minority member, my distinguished colleague the gentleman from California, Mr. Moorhead, as well as other subcommittee members—Mr. Morrison, Mrs. Schroeder, and Mr. Berman.

When Congress passed the wiretap law[1] in 1968, there was a clear consensus that telephone calls should be private. Earlier Congresses had reached that same consensus regarding mail and telegrams.

But in the almost 20 years since Congress last addressed the issue of privacy of communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically.

Today we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, lightweight compact television cameras for video surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago.

These new modes of communication have outstripped the legal protection provided under statutory definitions bound by old technologies. The unfortunate result is that the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the Government. Virtually every day the press reports on the unau-

---

[1] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510 et seq.

BEST COPY AVAILABLE

thorized interception of electronic communications ranging from electronic mail and cellular telephones to data transmissions between computers.

The communications industry is sufficiently concerned about this issue to have begun the process of seeking protective legislation. This bill is, in large part, a response to these legitimate business concerns.

The situation we face today was clearly foreseen by Justice Brandeis in 1928 when he said:

> The progress of science in furnishing the government with the means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[3]

Congress needs to act to ensure that the new technological equivalents of telephone calls, telegrams, and mail are afforded the same protection provided to conventional communications. It is my hope that in the weeks and months ahead the affected parties will work with the subcommittee in the spirit of cooperation and compromise to forge a bill which meets this urgent problem.

I would like to yield to my colleague, the gentleman from California.

Mr. MOORHEAD. Thank you, Mr. Chairman. I would like to commend you, Mr. Chairman, and your staff, and along with Senator Leahy and Senator Mathias and their staffs for developing this key initiative. I think it is clear that the need for legislation to ensure privacy in the dynamic area of communications has been well-recognized and well-documented both in the hearings held before this subcommittee last Congress as well as in hearings held before other subcommittees in both the House and the Senate.

As your remarks upon the introduction of H.R. 3378 indicate, you have worked carefully with the affected industries, the Department of Justice, and civil liberties groups in developing the legislation. This is significant for the days ahead. I am optimistic that each of these groups will, in turn, endorse H.R. 3378 which carefully balances the need for privacy against the legitimate interests of law enforcement.

In reviewing the legislation I was pleased to note that the bill leaves unchanged the carefully balanced provisions of the Foreign Intelligence Surveillance Act of 1978.

In any event, Mr. Chairman, I look forward to working closely with you and other members of the subcommittee toward the enactment of H.R. 3378.

I especially want to welcome our friend, Senator Pat Leahy, this morning to testify before us.

Mr. KASTENMEIER. I thank my colleague for his statements, and along with him I would also like to welcome my good friend and colleague, Senator Pat Leahy of Vermont. It is a great pleasure to do so.

Senator Leahy is vice chairman of the Senate Select Committee on Intelligence and ranking member of the Senate Subcommittee on Patents, Copyrights and Trademarks. Along with Senator

---

[3] *Olmstead* v. *United States*, 277 U.S. 438,474 (Brandeis, J., dissenting).

Charles McC. Mathias, he is a sponsor of the Senate bill S. 1667, which is identical to H.R. 3378. I have enjoyed working with him on this and other legislation to cope with the new technologies, such as our successful effort last year to grant protection to semiconductor chips.

Senator Leahy, we are delighted that you could be with us this morning. We are privileged to have you here. We have your statement; you may proceed from it if you wish—it is brief—or in any other fashion you care to.

Senator **Leahy**. Thank you. Could I ask John Podesta, our counsel, to come and join me at the table?

Mr. **Kastenmeier**. Mr. Podesta.

## TESTIMONY OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT, ACCOMPANIED BY JOHN PODESTA, COUNSEL

Senator **Leahy**. Mr. Chairman, I thank you for those kind words. It is an honor to be here with you and my good friend Congressman Moorhead. The three of us, along with Senator Mathias, have discussed this issue here on the Hill and other places around the country. It is something that has been a matter of interest to all of us. It truly is a privilege to be here.

As you know, we have joined with you and Congressman Moorhead to provide major privacy protection to new forms of electronic communication. Our bill, S. 1667, is identical to the bill you have introduced in the House. At this time of the year, nearing the end of the first session of the Congress, it helps things considerably to be moving on two fronts with identical bills.

I began working on the legislation over 1 year ago, when I wrote to the Attorney General to ask whether he believed interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap law. I received a reply from the Criminal Division of the Department of Justice which stated that Federal law protects electronic communications from unauthorized acquisition only where a reasonable expectation of privacy exists.

In a mastery of understatement, the Justice Department said:

> In this rapidly developing area of communications which range from cellular to cellular nonwire telephone connections to microwave-fed computer terminals, distinctions, such as (whether there does or does not exist a reasonable expectation of privacy) are not always clear or obvious.

Well, I didn't find that statement very informative. I didn't find it very reassuring, either. And more importantly, the American people and American businesses are no longer assured that the law protects their right to communicate privately.

Our primary wiretap law, title III of the Omnibus Crime Control and Safe Streets Act of 1968, fails to cover the unauthorized acquisition of data transmissions. That includes everything from interbank orders to private electronic mail hookups—some of the fastest growing areas of communications today.

When Congress enacted that law it had in mind a particular kind of communication—voice—and way of sending that communication—via common carrier analog telephone network. Only unauthorized "aural" acquisition of information was covered by by title

BEST COPY AVAILABLE

III. The Supreme Court has interpreted this to mean that in order to engender privacy protection, a communication has to be capable of being overheard. Data communications simply are not covered. The new technologies leave this statute hopelessly out of date.

There is no adequate legal protection against the unauthorized interception of data transmissions.

There is no adequate legal protection against the unauthorized interception of communications in private, noncommon carrier networks, even though these are proliferating everywhere, in every single State in the Union.

There is no adequate legal protection against the unauthorized access of electronic communications system computers to obtain or alter the communications contained in those computers.

There is no adequate legal protection afforded to cellular radio telephones, electronic pagers, and the private transmissions of video signals such as those used in teleconferencing, even if in that teleconference new discoveries or trade secrets are discussed.

Our bill is aimed at all these problems. It will go a long way toward providing the legal protections of privacy and security which are necessary to ensure the continued growth of new communications technologies. It will help protect private communications from interception by an eavesdropper, whether the eavesdropper is a corporate spy, a police officer without probable cause, or just a plain snoop.

Mr. Chairman, in the interest of time I am not going to recount the details of the bill. This will be included with my statement. But let me just say that we have worked hard over the past year, listening to all affected interests, to accommodate the legitimate needs of law enforcement while securing the privacy rights of users and operators of electronic communications systems.

And, Mr. Chairman, and Congressman Moorhead, I want to compliment you and your staff for the work already done.

There are a number of tough questions that have to be answered. I am hopeful that the hearings will provide these answers.

In closing, I would remind the committee that from the beginning of our history, first-class mail has had the reputation for preserving privacy, while at the same time promoting commerce. Both of these important interests must continue into our new information age. We cannot let any American feel less confident in putting information into an electronic mail network than he or she would in putting it into an envelope and dropping it off at the post office.

Thomas Jefferson once observed that "Laws and institutions must go hand in hand with the progress of the human mind * * * As new discoveries are made * * * institutions must advance also, and keep pace with the times." What Jefferson said 200 years ago is just as important today. There are a marvelous array of possibilities for better and faster communication worldwide, but we must keep faith with our 200-year history of privacy.

Protection of our communications privacy can go hand in hand with progress, but now is the time to make that a reality.

Mr. Chairman, again I compliment you and Mr. Moorhead and the subcommittee for the work you have done and for holding these hearings. I look forward to this legislation progressing in the Senate.

U.S. SENATOR PATRICK LEAHY

VERMONT

## Statement of Patrick Leahy
## on the Introduction of
## "The Electronic Communications Privacy Act of 1985"
September 19, 1985

Mr. President, for years this body has talked about the potential loss of personal privacy which could result from the electronic revolution. Today, I am introducing the "Electronic Communications Privacy Act of 1985" which aims at ending the talk and beginning the process of ensuring the privacy of communications of individual Americans and American businesses. I am very pleased to be joined in this effort by my distinguished colleague from Maryland, Senator Mathias.

Let me describe a problem that grows as we sit here.

At this moment phones are ringing, and when they are answered, the message that comes out is a stream of sounds denoting one's and zero's. Nothing more. I am talking about the stream of information transmitted in digitized form, and my description covers everything from interbank orders to private electronic mail hookups.

By now this technology is nothing remarkable. What is remarkable is the fact that none of these transmissions are protected from illegal wiretaps, because our primary law, passed back in 1968, failed to cover data communications, of which computer-to-computer transmissions are a good example.

When Congress enacted that law, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, it had in mind a particular kind of communication--voice--and a particular way of transmitting that communication--via a common carrier analog telephone network. Congress chose to cover only the "aural acquisition" of the contents of a common carrier wire communication. The Supreme Court has interpreted that language to mean that to be covered by Title III, a communication must be capable of being overheard. The statute simply fails to cover the unauthorized interception of data transmissions.

Similarly, there is no adequate federal legal protection against the unauthorized access of electronic communications system computers to obtain or alter the communications contained in those computers.

Problems also exist with regard to the legal protection afforded to cellular radio telephones, electronic pagers and the private transmissions of video signals such as that used in teleconferencing.

There may have been a day when good locks on the door and physical control of your own papers guaranteed a certain degree of privacy.

But the new information technologies have changed all that.

Hearings in the last Congress held by Senator Mathias and myself in the Senate Judicary Committee and by Congressman Robert Kastenmeier in the House Judiciary Committee clearly demonstrate the scope of these problems and the need to act.

Congressman Kastenmeier, Senator Mathias and I have been working for over a year with the Justice Department and many individuals, businesses and industry groups who are concerned with updating the law to better protect communications privacy.

The product of that effort is the bill which Senator Mathias and I are introducing today. Congressman Kastenmeier is introducing identical legislation in the House.

The Electronic Communications Privacy Act of 1985 contains a number of important changes:

-- The Act amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968--the federal wiretap law.

-- Definitions contained in Title III are amended to broaden protection from only voice transmissions to all electronic communications including data and video carried on non-public systems. The requirement that to fall within the coverage of Title III an interception has to be by "aural acquisition", is dropped.

-- Protection of only common carrier telephone systems is broadened to include all electronic communications systems unless designed to be accessible by the public.

-- The bill contains criminal penalties for unathorized access to the computers of an electronic communication system, if messages contained therein are obtained or altered. If done for commercial gain or for malicious reasons, the crime could be prosecuted as a felony offense.

-- To obtain communications contained in the computers of an electronic communication system, such as an electronic mail service, the government would be required to obtain a warrant based on a probable cause standard.

-- An operator of an electronic communications system is restricted from disclosing the contents of an electronic message except in specified circumstances or unless authorized by the person sending the message.

-- An electronic communications system and the users of the system are granted a federal cause of action to seek civil damages for violation of any of the rights contained in the Act.

-- Finally, the bill provides that law enforcement agencies must obtain a court order based on a reasonable suspicion standard before installing a pen register or being permitted access to records of an electronic communications system which concern specific communications.

The bill does not affect the carefully balanced provisions governing foreign intelligence surveillance contained in the Foreign Intelligence Surveillance Act of 1978.

These changes will go a long way towards providing the legal protections of privacy and security which the new communications technologies need to flourish.

As I said earlier, we have worked hard over the past year to listen to all affected interests and to accommodate the legitimate needs of law enforcement while securing the privacy rights of users and operators of electronic communications systems.

A number of tough questions remain to be answered. Chief amongst these is whether electronic communications systems which are not designed to protect the privacy of the communications being carried should be afforded legal protection.

But raising this question should in no way suggest that communications privacy is just an industry problem.

It is no solution to say that anybody concerned about the privacy of these communications can pay for security by paying for encryption.

Encryption can be broken. But more importantly, the law must protect private communications from interception by an eavesdropper, whether the eavesdropper is a corporate spy, a

POLICE OFFICER WITHOUT PROBABLE CAUSE OR JUST A PLAIN SNOOP.

UNAUTHORIZED ACQUISITION OF INFORMATION IS NOT JUST A THEORETICAL PROBLEM, OR ONE CONFINED TO HARMLESS TEENAGE HACKERS. COMMUNICATIONS COMPANIES HAVE BEEN FACED WITH GOVERNMENT DEMANDS, UNACCOMPANIED BY A WARRANT FOR ACCESS TO THE MESSAGE CONTAINED IN ELECTRONIC MAIL SYSTEMS. AND THE UNWANTED PRIVATE INTRUDER, WHETHER A COMPETITOR OR A MALICIOUS TEENAGER, CAN DO A GREAT DEAL OF DAMAGE BEFORE BEING, OR WITHOUT BEING, DISCOVERED.

FROM THE BEGINNING OF OUR HISTORY, FIRST-CLASS MAIL HAS HAD THE REPUTATION FOR PRESERVING PRIVACY, WHILE AT THE SAME TIME PROMOTING COMMERCE.

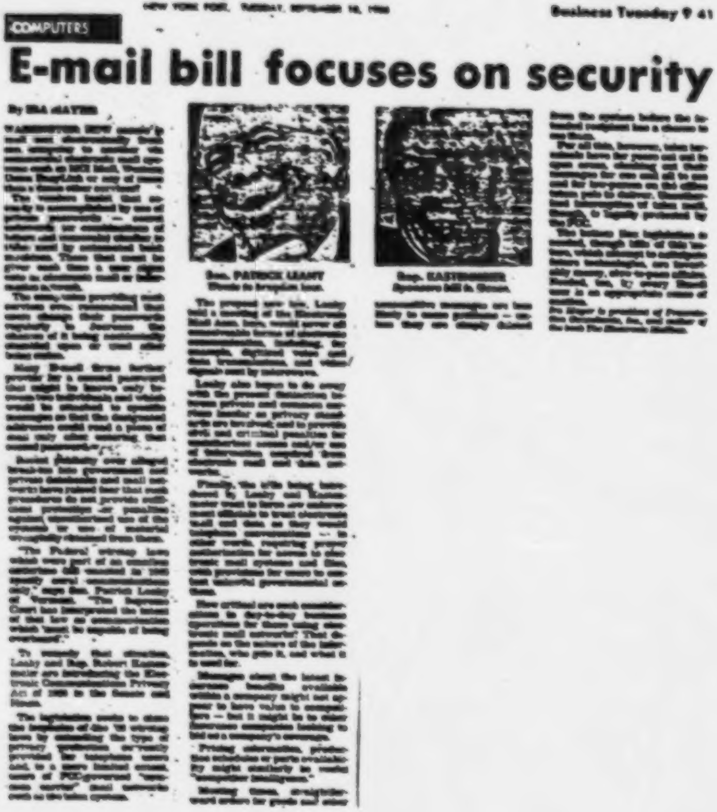
BOTH OF THESE IMPORTANT INTERESTS MUST CONTINUE INTO OUR NEW INFORMATION AGE. WE CANNOT LET ANY AMERICAN FEEL LESS CONFIDENT IN PUTTING INFORMATION INTO AN ELECTRONIC MAIL NETWORK THAN HE OR SHE WOULD IN PUTTING IT INTO AN ENVELOPE AND DROPPING IT OFF AT THE POST OFFICE.

THOMAS JEFFERSON ONCE OBSERVED THAT, "LAWS AND INSTITUTIONS MUST GO HAND-IN-HAND WITH THE PROGRESS OF THE HUMAN MIND....AS NEW DISCOVERIES ARE MADE...INSTITUTIONS MUST ADVANCE ALSO, AND KEEP PACE WITH THE TIMES."

AMERICAN BUSINESSES HAVE PRODUCED A MARVELOUS ARRAY OF POSSIBILITIES FOR BETTER AND FASTER COMMUNICATION WORLDWIDE. NOW IS THE TIME FOR OUR LEGAL INSTITUTIONS TO ALSO ADVANCE AND KEEP PACE WITH THE TIMES.

THE PROTECTION OF COMMUNICATIONS PRIVACY CAN GO HAND-IN-HAND WITH PROGRESS. OUR JOB IS TO MAKE BOTH A REALITY. NOW IS THE TIME TO ACT.

I ASK UNANIMOUS CONSENT THAT A SUMMARY OF THE BILL AND ITS TEXT BE PRINTED IN THE RECORD AT THIS POINT.



NEW YORK POST, TUESDAY, SEPTEMBER [illegible]

Business Tuesday 9 41

COMPUTERS

# E-mail bill focuses on security

By [illegible]

[illegible]

Sen. PATRICK LEAHY

[illegible]

Rep. KASTENMEIER

Sponsors bill in House.

[illegible]

# New Law to Protect Computer Data Sought

Special to The New York Times

WASHINGTON, Sept. 18 — Computerized information would gain legal protection from unauthorized access or interception under legislation that Representative Robert W. Kastenmeier and Senator Patrick J. Leahy plan to introduce Thursday.

The two lawmakers said today that a change in existing law was essential to protect the privacy of individual citizens, business organizations and other institutions that are increasingly transmitting and storing information in computerized form.

"The technological changes of the last decade have severely affected the privacy protection afforded to individual Americans and American businesses," said Mr. Leahy, a Vermont Democrat who is a member of the Senate Judiciary Committee.

Because of gaps in the wiretapping provisions of the Omnibus Crime Act of 1968 and other laws, computerized information does not enjoy the same kinds of legal protection as do older forms of communications such as telephone conversations or first-class letters.

## Working With Reagan Aides

The staffs of both Mr. Kastenmeier and Mr. Leahy have been working with Reagan Administration officials and communication industry executives to develop provisions that would find wide acceptance.

"We have worked out a lot of problems and I'm optimistic we can develop a final compromise," said Cary Copeland, an official in the Justice Department office that works on legislation.

Representative Kastenmeier, a Wisconsin Democrat who is chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, said many new technologies have become widely used in the 17 years since Congress passed a

THE NEW YORK TIMES, THURSDAY, SEPTEMBER 19, 1985 A18

comprehensive communication privacy law.

"Today we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, lightweight, compact television cameras for video surveillance and a dazzling array of digitized information networks which were little more than concepts two decades ago," Mr. Kastenmeier said.

Michael F. Cavanagh, executive director of the Electronic Mail Association, whose members include industry giants such as the ITT Corporation, the International Business Machines Corporation and the GTE Corporation, said his group was pleased by the work done so far on the proposal. "We hope that we can work out a final version that will directly deal with the problems of both the unauthorized access to data bases and the illegal interception of computerized information," he said.

Among the major provisions of the proposal is one that would extend the current restrictions of law protecting telephone conversations to all forms of electronic communication. At present, it is a crime for anyone to eavesdrop on a telephone conversation except a law-enforcement official who has obtained an order from a special court.

A second provision would require a law-enforcement agency to obtain a court order before it could gain access to the records held in an electronic communication system operated by an organization such as a credit card company or electronic mail service that offers businesses computer space in which to store their records.

Mr. Kastenmeier said the current legal deficiencies were exacerbated by the rapid change in the amount and types of governmental surveillance. In 1984, for example, the Federal Government undertook more wiretaps and bugs than in any year since 1973.

Mr. Kastenmeier said a recent study by Congress's Office of Technology Assessment had found that 29 different Federal agencies were using or planned to use television surveillance, 21 were using or planned to use radio scanners, 6 were conducting cellular telephone interceptions and 15 were employing various kinds of personal tracking devices.

EVERY DROP COUNTS: SAVE WATER

STROM THURMOND, S.C., CHAIRMAN
CHARLES McC. MATHIAS, JR., MD.
PAUL LAXALT, NEV.
ORRIN G. HATCH, UTAH
ROBERT DOLE, KANS.
ALAN K. SIMPSON, WYO.
JOHN EAST, N.C.
CHARLES E. GRASSLEY, IOWA
JEREMIAH DENTON, ALA.
ARLEN SPECTER, PA.
JOSEPH R. BIDEN, JR., DEL.
EDWARD M. KENNEDY, MASS.
ROBERT C. BYRD, W. VA.
HOWARD M. METZENBAUM, OHIO
DENNIS DeCONCINI, ARIZ.
PATRICK J. LEAHY, VT.
MAX BAUCUS, MONT.
HOWELL HEFLIN, ALA.
VINTON DeVANE LIDE, CHIEF COUNSEL AND STAFF DIRECTOR
DEBORAH K. OWEN, GENERAL COUNSEL
SHIRLEY J. FANNING, CHIEF CLERK
MARK H. GITENSTEIN, MINORITY CHIEF COUNSEL

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, D.C. 20510

January 26, 1984

The Honorable William French Smith
Attorney General of the United States
Department of Justice
10th Street and Constitution Avenue, N.W.
Washington, D.C. 20530

Dear Attorney General Smith:

Recent newspaper and magazine articles have focused public debate on the question of whether federal government law enforcement agents may, as a matter of law, secretly and without a warrant or court order employ electronic surveillance of wire communication that does not involve the "aural acquisition" of information. (See, e.g., enclosed published materials.) Such communication would include, but would not be limited to, digital communication and any form of "pen register" or "touch tone decoder" device which is used to acquire from the contents of a wire communication the identities or locations of the parties to the communication, but which has been held to be outside the protections of the Fourth Amendment as well as the coverage of Chapter 119 of Title 18 of the United States Code (Chapter 119).

From published articles it would appear that the Deputy Assistant Attorney General for the Criminal Division has expressed some public views on this subject. According to reports he has indicated that as a matter of policy, in many cases the Department would advise seeking a warrant or court order. However, he did not appear to conclude that there was currently a statutory requirement for a warrant or court order to conduct electronic surveillance involving nonaural acquisitions.

On the other hand, there has been reported a contrary view of a Senate expert that the Foreign Intelligence Surveillance Act of 1979 (FISA) criminalizes the conduct of all such wiretaps -- whether for domestic law enforcement or foreign surveillance -- if conducted without warrant or court order. The argument is based on the provisions of section 109 of FISA, 50 U.S.C. 1809. That section makes it an offense to engage in electronic surveillance under color of law except as authorized by statute. The argument maintains that the nonaural electronic surveillance at issue falls within the definition of electronic surveillance in FISA and that Chapter 119 does not specifically provide a statutory exception for nonaural communication even though that section by its own terms does not make nonaural interception subject to that chapter's legal requirements.

. . .

In light of these inconsistent views of current statutory requirements, an attorney from my staff contacted the Department of Justice to ascertain whether the views of the Department were correctly reported and if not, what were those views. Apparently, the matter is currently under consideration, and the Department's answer is expected shortly. I currently am reviewing this question and would very much appreciate receiving the Department's written views on this question as expeditiously as possible.

Thank you for your attention to this matter.

Sincerely,

PATRICK LEAHY
United States Senator

PJL:mn

Enclosure

U.S. Department of Justice

Criminal Division

Assistant Attorney General

Washington, D.C. 20530

MAR 9 1984

Honorable Patrick Leahy
United States Senate
Washington, DC 20510

Dear Senator Leahy:

The Attorney General has asked me to reply to your letter of January 26, 1984, concerning the Department of Justice's views on the question whether federal law enforcement officials may, as a matter of law, conduct warrantless electronic surveillance of wire communications when the surveillance does not involve the aural acquisition of the contents of such communications.

As you know, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. Sections 2510-2520 (Title III) does not govern the electronic and mechanical interception of wire and oral communications unless the interception accomplishes "the aural acquisition of the contents" of the communication. 18 U.S.C. Section 2510(4). As the legislative history of Title III makes clear, that statute "protect[s] the privacy of the communication itself and not the means of communication." S. Rep. No. 1097, 90th Cong., 2d Sess., 90 (1968), reprinted in [1968] U.S. Code Cong. & Admin. News, pp. 2112, 2178. The Supreme Court has recognized that interceptions that do not secure the "aural acquisition" of the contents of a communication, and thus do not "overhear" the substance of a conversation, are not within the scope of Title III. United States v. New York Telephone Co., 434 U.S. 159, 166-168 (1977).

Nonaural interceptions of wire communications, while not within the purview of Title III, may, in certain instances, be regulated by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. Sections 1801-1811 (FISA). Although the procedural provisions of FISA apply to electronic surveillance within the United States for foreign intelligence, and not for domestic law enforcement purposes, the definitional and criminal penalties provisions of the act appear to have a broader applicability. The procedural requirements of FISA specifically attach only to electronic surveillance, as defined in that act, when the surveillance is employed for the purpose of obtaining foreign intelligence information, but the criminal penalties section of FISA is nowhere limited to the intelligence gathering function. That section states that a person is guilty of an offense if he intentionally engages in "electronic surveillance" under color of law except as authorized by statute. 50 U.S.C. Section 1809(a)(1). An affirmative defense is provided for law enforcement officers who engage in electronic surveillance pursuant to a search warrant or court order. 50 U.S.C. Section 1809(b).

Since FISA requires a court order, but not a warrant, Congress presumably would not have made the defense applicable to law enforcement officers acting pursuant to both court orders and warrants had it not intended that the criminal sanctions apply to electronic surveillance beyond the foreign intelligence gathering area. Support for this position is found in the House Conference Report on the bill that eventually became FISA wherein it was noted that House amendments to the bill "provide for separate criminal penalties in this act, rather than by conforming amendments to Title 18, for any person who intentionally engages in electronic surveillance under color of law except as authorized by statute. A defense was provided for a defendant who was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction." House Conf. Report No. 95-1720, 95th Cong., 2d Sess., 33 (1978), reprinted in U.S. Code Cong. & Admin. News p. 4062 (emphasis added). We would conclude, therefore, that a court order or warrant must be obtained whenever a surveillance technique employed in a domestic criminal investigation falls within FISA's definition of "electronic surveillance."

We do not believe, however, that 50 U.S.C. Section 1809 constitutes a statutory prohibition against all warrantless electronic surveillance involving nonaural acquisitions of communications because FISA's definition of "electronic surveillance" does not apply to all such communications. "Electronic surveillance," as defined in FISA, includes:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. Section 1801(f). All the definitions of "electronic surveillance" quoted above, except for subsection 1801(f)(2) limit the term by making it applicable when there exists "a reasonable expectation of privacy." Subsection 1801(f)(2) applies more broadly to a "wire communication," which is defined as "any communication while it is being carried by wire, cable, or other like connection." 50 U.S.C. Section 1801(1) (emphasis added).

As you probably know, however, many long distance calls today are transmitted partly by wire and partly by radio communications, and it appears that a warrant is not required for the nonaural interception of the radio or microwave portion of a combined wire-radio transmission. This is so because the radio or microwave portions of such communications are not governed by Section 1801(f)(2). They fall within either Section 1801(f)(1) or 1801(f)(3), both of which define "electronic surveillance" in terms of an individual's expectation of privacy in the communication intercepted. As the Senate Report explains:

> Because most telephonic and telegraphic communications are transmitted at least in part by microwave transmissions, subdefinition [2] is meant to apply only to those surveillance practices which are effected by tapping into the wire over which the communication is being transmitted. The interception of the microwave radio transmission is meant to be covered by subdefiniton [3] . . . or by subdefinition [1] . . .

S. Rep. No. 604, 95th Cong., 2d Sess., 33 (1977), *reprinted in* [1978] U.S. Code Cong. & Admin. News, pp. 3904, 3934.

Thus, the question whether a warrant or court order is legally required to conduct a nonaural interception of the radio portion of a hybrid wire-radio communication is, in our view, dependent upon whether there exists a reasonable expectation of privacy on the part of the individual whose communications are to be intercepted. If there exists such an expectation, a search warrant or court order is clearly necessary. If however, the individual can claim no such justifiable privacy expectation in the communication, neither FISA nor the Fourth Amendment prohibits the warrantless interception of that communication. See *Katz* v. *United States*, 389 U.S. 347 (1967); *Smith* v. *Maryland*, 442 U.S. 735, 740-741 (1979).

In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as that set out above are not always clear or obvious. Consequently, while we do not believe that there is currently a statutory requirement that a court order or search warrant be obtained in *all* instances involving nonaural interception, it is the policy of the Department of Justice to obtain such an order or warrant when nonaural electronic surveillance techniques are employed and our analysis indicates there is a reasonable expectation of privacy.

We hope that this letter has clarified the Department's position with respect to the current legal requirements for nonaural interceptions. However, if we can be of any further assistance, please do not hesitate to contact me.

Sincerely,

Stephen S. Trott
Assistant Attorney General
Criminal Division

By:
John C. Keeney
Deputy Assistant Attorney General
Criminal Division

**U.S. Department of Justice**

Criminal Division

*Office of the Assistant Attorney General* *Washington, D.C. 20530*

JUN 14 [illegible]

Honorable Patrick Leahy
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

By letter dated March 9, 1984, the Department of Justice responded to your letter concerning warrantless electronic surveillance of wire communications when the surveillance does not involve the aural acquisition of the contents of such communications. On the third page of our response, we suggested that "many long distance calls today are transmitted partly by wire and partly by radio . . . and it appears that a warrant is not required for the nonaural interception of the radio or microwave portion of a combined wire-radio transmission."

We wish to make clear that we believe that the microwave radio portion of a telephone call is normally accompanied by a justifiable expectation of privacy. Consequently, a judicial warrant would be required for the nonconsensual interception of such calls.

We regret any confusion created by our former letter.

Sincerely,

STEPHEN S. TROTT
Assistant Attorney General
Criminal Division

By: John C. Keeney
JOHN C. KEENEY
Deputy Assistant Attorney General
Criminal Division

Mr. **Kastenmeier**. Well, I commend you, Senator Leahy, for your leadership in this field and the work that has led up to this introduction.

I have a question or two and I will be very brief. As a former prosecutor, former vice president of the National District Attorneys Association, and also as vice chairman of the Intelligence Committee of the Senate do you feel that the bill as proposed is consistent with the Foreign Intelligence Surveillance Act, in terms of balancing the legitimate interests of both law enforcement and privacy to the extent that it is possible?

Senator **Leahy**. On the latter part, we have looked at it through FISA and I feel that FISA protects our legitimate foreign policy, intelligence, and counterespionage considerations. I know, Mr. Chairman, you are also a member of HPSCI—the House Intelligence Committee—and I think what I could say in an open session is I think our interests are well protected. I mean our legitimate national interests as well as the interests that we have always protected under FISA of Americans' right of privacy.

In the law enforcement arena, yes, I think that it does take into consideration legitimate interests. You know, when we considered the question of wiretapping, in the first place, we had to go through this discussion of balancing American citizens' interests and legitimate interests of law enforcement. We basically took the approach that we take in any kind of a search-and-seizure question. We know that our homes are sacrosanct, our businesses are sacrosanct; and if the law enforcement want to go in there, they do it only with probable cause and a warrant. The original wiretap legislation required that.

Now we have gone to a new way of communication the rights of privacy—the anticipation of privacy—of Americans is still the same. And to the extent that law enforcement is going to have to intercept those things, they must do it with probable cause and with appropriate warrant.

The rules don't change at all. The technology changes. All the legislation does is to make sure that the rules stay consistent with the technology.

Mr. **Kastenmeier**. I understand.

The gentleman from California.

Mr. **Moorhead**. I just wanted to indicate I think we are going to have the support of the Attorney General's Office——

Senator **Leahy**. I think we will.

Mr. **Moorhead** [continuing]. In spite of the letter. And there may have to be a minor amendment here or there that we didn't think of in advance, but I think we will produce a good bill and it will get through.

One of the major newspapers in Los Angeles has been editorializing on this problem for some time. I believe that people throughout the country will be happy to get rid of the kinds of eavesdropping on cellular phone calls and other things that really are no one else's business but the people who are making the calls.

Mr. **Kastenmeier**. One last question I have is, Can you share with us any information or intelligence on what plans you and Senator Mathias might have for processing this or similar legislation?

Senator **Leahy**. Chairman Mathias and I hope to have hearings by the end of October and to move forward as quickly as we can. I don't know how long we are going to be in session this year. The tax bill and other agenda items will affect that. I would hope, though, that we could have a subcommittee markup on S. 1667 before Thanksgiving. I don't know if this is realistic, but certainly we will have our hearings before then.

To the extent that both bodies can concur on a basic package, this legislation could move very rapidly.

Mr. **Kastenmeier**. Well, that is good news.

Again, we are very indebted to you for coming over from the Senate and sharing with us your views on this important question. Thank you, Senator Leahy.

Senator **Leahy**. Thank you, Mr. Chairman.

Mr. **Kastenmeier**. The committee, because there is a vote on in the House, will be in recess for about 10 minutes, after which time we will call on Mr. Walker, who is our next witness. Until then, the committee stands in recess.

[Recess.]

Mr. **Kastenmeier**. The committee will be in order.

Our next witness in this morning's hearings is Philip Walker, general regulatory counsel to GTE Telenet Inc. and vice chairman of the Electronic Mail Association. Mr. Walker is one of the founders of Telenet and is coauthor of a book, "Computers and Telecommunications: Issues in Public Policy." He brings us the benefit of both legal and technical expertise. He holds a B.S. in electrical engineering from Yale; an M.S. in management from M.I.T.; and a J.D. from Georgetown.

Mr. Walker, we have your statement. You may proceed as you wish. Actually your statement is only five pages long, so if you would just care to read it, that would be fine. We are glad to have you here, Mr. Walker.

## TESTIMONY OF PHILIP M. WALKER, GENERAL REGULATORY COUNSEL, GTE TELENET INC., AND VICE CHAIRMAN, ELECTRONIC MAIL ASSOCIATION, ACCOMPANIED BY MICHAEL F. CAVANAGH, EXECUTIVE DIRECTOR, ELECTRONIC MAIL ASSOCIATION

Mr. **Walker**. Thank you, Mr. Chairman.

We appreciate the opportunity to appear this morning. As you noted, I am appearing on behalf of the Electronic Mail Association, and I have with me this morning Michael Cavanagh, the association's executive director, who has been very active in working on this area.

First, I think it might be helpful to provide a little background on the Electronic Mail Association and the electronic messaging industry.

The Electronic Mail Association is a Washington-based trade association created 2 years ago by several of the leading firms in the industry. We now have over 60 members spread across the United States and Canada; and in Europe as well. Our board of directors includes firms such as GTE, ITT, Western Union, MCI, IBM, Digital Equipment, and Citibank.

A major part of our mandate is to address key policy issues facing the burgeoning electronic mail industry, and it certainly I think is fairly obvious that privacy and security are right at the head of that list.

Electronic mail is a product, an application, of the melding of computer and communications technology. It allows virtually instantaneous communication with similarly equipped users around the globe. In addition to speed, electronic mail is useful because it permits a user to send a message to a friend or colleague even when the recipient is not available at his or her desk. When the recipient returns from a meeting, from lunch, or whatever, he will find the message in his electronic mailbox.

Also, the message, be it a few words or a lengthy document stored in computer memory, can be sent to one recipient or simultaneously to literally hundreds of recipients with the push of a button.

With the rapid proliferation of personal computers, communicating word processors, and so forth, it is easy to understand why the industry is growing at a rapid rate.

Most industry analysts estimate that the computer-based messaging industry has around $250 million of annual revenues at the present and will grow to the range of $2 to $3 billion in annual revenues by the early 1990's. There are currently several hundred million messages sent annually. This figure will grow into the tens of billions in less than a decade. It is reasonable to assume that during the 1990's electronic mail will become a regular and important part of the communications mix that a substantial number of Americans use in their workplace, and also increasingly at home as well.

Mr. Chairman, with those comments as a preface to underscore the importance of this subject, let me say on behalf of the Electronic Mail Association that we would like to commend you and Senator Leahy for developing this vitally important legislation.

We believe that the measure, as introduced, deals with the key concerns regarding electronic mail privacy and security that need congressional action. We were pleased to make recommendations to you and your staff during the drafting process for this bill, and we hope to be of assistance as the measure moves through the legislative process. We have distributed the bill to our membership, and will report any detailed comments from our members to the staff.

Mr. Chairman, H.R. 3378 goes to the heart of the electronic mail concerns by prohibiting unauthorized access to electronic communications systems. This is essential since the most likely method of privacy invasion comes when someone attempts to enter an electronic mailbox of a system user without proper authorization. Messages are sitting in the computer waiting properly authorized access by the recipient. Just as letters sitting in conventional mailboxes at the curbside are afforded legal protection, we strongly believe the public has a right to privacy for their electronic messages as well.

The bill you and Senator Leahy have introduced provides a structure encompassing several different levels of civil and criminal penalties for privacy violations. We believe this differentiation makes sense for it can provide for appropriately heavy penalties for cases of corporate espionage, while permitting lesser sanctions against the stereotypical young hacker. The bill does make clear, however, that a youngster with a personal computer is committing a crime when he or she violates someone's privacy, just as if they stole the contents of someone's conventional mailbox.

We also wholeheartedly endorse the concept of recovery of civil damages which is incorporated in the bill. Citizens who have had their right of privacy violated should have the opportunity to sue the guilty parties. We see this as potentially an outstanding deterrent as well.

The bill includes a provision which prohibits employees of service providers from divulging the contents of any communication which they might inadvertently gain awareness of. We support this concept. It tracks similar provisions which have been in effect in the telephone and telegraph industries for decades. However, we are unclear at this point whether section 705 of the Communications Act, or your bill, would apply to the subpoena of electronic messages in certain civil lawsuits. This may be simply a matter of clarification, which we will undertake to resolve with your staff.

Mr. Chairman, you have highlighted the need for legal mechanisms to be established to regulate Government access to electronic mail messages. We concur since at the present time companies in our industry are faced with no clear standards when Government agencies seek access to subscriber information. This has not, as yet, become a common occurrence, but without congressional action the uncertainty will continue. We believe the approach taken in your bill is a sound one since it establishes clear procedures, just as procedures currently exist for telephone wiretaps and for surveillance of U.S. postal mail.

We also agree with the provision mandating that this legislation will cover any provider of electronic communications service, not just communications common carriers. As you know, the Federal Communications Commission has defined electronic mail as an "enhanced service," not subject to common carrier regulation.

Also, electronic mail systems are widely operated by corporations, nonprofit organizations, and Government agencies for their own internal use. During the next decade these various discrete systems will increasingly become interconnected with each other. Electronic mail users obviously deserve privacy protections regardless of what type of entity runs their system.

In summary, the Electronic Mail Association believes this is truly landmark legislation. Chairman Kastenmeier, we wish to commend you, Senator Leahy, and your cosponsors for taking the initiative on a subject that will be ever more important to the American public in the years ahead. We strongly support your efforts and we would only hope that with such a fine starting point final passage can be achieved during the present Congress.

Thank you.

Mr. KASTENMEIER. I share that hope. And thank you very much for that concise but clear statement, and a very useful one I might add. In fact, if anything, the complexity of the subject and speculation about the applicability of it is such that it probably doesn't impinge on certain areas which we might later want to discuss.

But let me at the outset ask you several questions for background for the hearings. With respect to the interception of electronic mail today, what do you understand to be the current Federal and State law? Please generalize; I guess it would be a little hard to be specific with reference to every State.

Mr. **Walker**. I can generalize by saying that unfortunately it is rather murky at this point. There is no clear Federal law that would prohibit that interception in all cases. Section 705 of the Communications Act may apply in certain instances to interception of a message in transit, but does not appear to apply to unauthorized access to the message once it has been received and is stored in the computer's memory bank. And that frankly is where most of the unauthorized access problems have arisen.

There are other Federal statutes that may apply in certain instances, but frankly it is unclear in many cases and, as a result, it has been difficult sometimes to obtain a basis for prosecution in an instance where the Government clearly wishes to bring a criminal prosecution. They need a basis for that.

At the State level, some States in the last several years have adopted, enacted computer crime laws which may apply to interception or unauthorized access to electronic messages. But those are not uniform. A number of States have no such legislation at all. So, you end up with sort of a crazy patchwork quilt of legislation depending on the jurisdiction. And that is particularly important when you consider that electronic mail by its nature is typically an interstate-type of activity. You will have the computer in one State, the sender of the message in a second State, and the recipient or recipients in any number of additional States. So, trying to get a local prosecutor to bring an action under State law, even if there is a State law, in one of those States may be very difficult.

Mr. **Cavanagh**. Mr. Chairman, could I, also, in relation to that?

Mr. **Kastenmeier**. Of course. We are pleased, Mr. Cavanagh, to have your comments.

Mr. **Cavanagh**. The additional problem with the question of the electronic mail technology is, in fact, even if a sender and a recipient are across the street, as Mr. Walker says, the computer could be in another State. But also, we may well have someone sending that message not from his home or his office, but rather while they are attending a business meeting in another State and sending it to the recipient who will not be receiving it at their home or office location as well, but may be accessing it someplace else. So, it is extremely difficult to deal just with a State law in this respect we think.

Mr. **Walker**. Mr. Chairman, one other point occurred to me that I think is important to note. And that is, on the civil side of things the bill establishes a civil right of action to provide a means of redress for privacy violations in this area. That to my knowledge is not presently available at all as a general matter, and I think it will be very important both as a supplement to the possibility of criminal prosecution and also to provide an independent avenue for redress.

Mr. **Kastenmeier**. What other differences or advantages might this bill have as you see it as compared to the narrower, so-called computer crime bills? There was, of course, a very limited form of a computer crime bill enacted in the 98th Congress which is currently law, although its scope is not general and certainly not commercial. I think for comparative purposes it might be useful for your comment, Mr. Walker, or that of Mr. Cavanagh's, on the subject.

Mr. WALKER. Well, Mr. Chairman, I think this bill might properly be viewed as complementary to the computer crime bills that we have seen. As you mentioned, the bill that was passed last year does not cover all computer systems. Its scope is narrowly focused. It covers Federal Government systems, it covers systems operated by certain financial institutions, for example; but, in general, private sector computers are not covered. And that is where, of course, our industry operates. So, on the Federal side current existing computer crime legislation is not all-encompassing in terms of the systems covered.

Second, of course, it does not cover interceptions of messages in transit. The computer crime legislation deals with unauthorized penetration of the computer only, as I recall it.

Third, it is not clear in all instances that a mere interception or reading of a message would trigger an offense under some of that legislation. I am speaking now particularly at the State level. If there has been some malicious damage done or something of that sort, then clearly it would be covered. But under some of those bills it is possible, as I understand it, that a mere reading of a message or interception of a message might not be covered.

So, if you look at it from the standpoint of privacy protection, those bills may miss the mark. That is why I say it seems to me this bill and the computer crime legislation are complementary to each other. I wouldn't think that either one alone would be sufficient.

Mr. KASTENMEIER. Do you think—I don't know whether you discussed that point—whether or not the term "electronic communication service provider" is defined clearly enough? As you say, it must go beyond common carriers to be effective. But should we attempt to be specific in our definition of "electronic communication service providers"? Do we know what is included and what is not?

Mr. WALKER. We are quite satisfied with the definition contained in the bill. It is a general definition, and by its nature would then encompass a system operated by a commercial company for hire; a private commercial system, such as one that a corporation might operate for its own in-house employees; a Government agency; a nonprofit organization, such as a university or something like that which markets access to outsiders. So, we feel that the scope of the definition is appropriate.

Mr. KASTENMEIER. My question derives from that, perhaps, but is larger conceptually. Looking at history, is the bill broad enough in terms of future technology or developments in technology so as to comprehend that which reasonably might eventuate in the next few years or a decade or so; or is it vulnerable to obsolescence even as the 1968 law has proved to be?

Mr. WALKER. Well, I wouldn't presume to speak for all aspects of the communication industry. But from the perspective of the electronic mail industry, I think it will survive a test of time because of the fact that it is written in a general way that applies to all electronic communications and applies to both interception and unauthorized access. As clear as our crystal ball is at this point, I can't—or as murky as it may be, I can't envision a privacy invasion that didn't involve either an unauthorized interception or an unauthorized access.

Mr. **Kastenmeier**. One other question. It is easy when you are dealing with wiretapping in terms of the old technology. When you wiretap you really are aggressively attempting to intercept that which is intended to be private. It is easy to contemplate the difference with the old party telephones where you would hope your conversation would be private but your expectation is conditioned by the knowledge that your neighbors are on the line.

With that as sort of historical background, my question is what about inadvertent interception? Is the new technology so pervasive and ubiquitous that inadvertent interceptions are common and the test of who is violating this privacy becomes somewhat murky as compared to an earlier time where one needed to be more aggressive in terms of the interception and violation of privacy?

Mr. **Walker**. Well, again from the perspective of the electronic mail field, I don't believe that the possibility of inadvertent interception is anywhere near so great that that would be a concern. I think that the way these electronic mail systems are operated the user first of all will access the computer over some form of a dedicated channel, be it a dial-up telephone line or an in-house communications link, say, within a corporate office complex, or something like that. And normally one could not intercept communications across that line without intentionally doing so, wiretapping if you will.

I am talking now the authorized user. Once he accesses the computer, let's say that a message is going to be transmitted to a second user; the sender will enter the message into the computer using a specific mailbox address for the recipient, and that will go into a computer file earmarked for the recipient, which is protected with passwords and so forth. So that again no one but that recipient could access that file unless someone tried, intentionally tried to evade those safeguards.

Mr. **Cavanagh**. Perhaps the password could be considered similar to sealing the envelope when you send first-class mail. There clearly is an action there that does suggest privacy.

Mr. **Kastenmeier**. I appreciate that response because I think you know what the background of the question is. It is not clear sometimes within systems. If you intend an electronic message for A, but B is in the same complex and uses the same computer system, whether or not B—possibly even in the same office—may inadvertently enter somebody else's mailbox would be a legitimate question, whether we are protecting discretely intended messages or otherwise.

Well, thank you.

I would like to yield to my colleague from California.

Mr. **Moorhead**. Thank you, Mr. Chairman.

And I want to thank you, Mr. Walker, for your expertise on the subject, which has been very helpful.

Do you believe that the civil and criminal penalties in this legislation are sufficient to handle the problems?

Mr. **Walker**. Well, as far as we can tell at this point, I think they are. They represent a giant step forward from where we are today and provide a graduated range of responses depending upon the nature of the problem. For example, on the civil side you have fairly minimal statutory penalties ranging up to on the upper end a fairly sizable statutory amount and the opportunity for actual damages, so that you can cover a spectrum of different types of offenses very appropriately.

Mr. **Moorhead**. You indicate on page 4 of your statement that it has not become a common occurrence for the Federal Government, or its agencies, to seek access to subscriber information. When they have done so, have they sought to get the information through a warrant or have they just plowed in to get it?

Mr. **Walker**. Well, I am personally only aware of one instance that has been brought to our attention involving a public electronic mail provider. And in that instance I believe that the company was served with a subpoena by the law enforcement authorities.

Mr. **Moorhead**. That approach, going through the courts and getting a subpoena, would still be available if they were working on a——

Mr. **Walker**. Yes; what the bill does is provide a clearer standard that must be met by Government in order to obtain that court order. A standard that, as I understand it, is not presently in existence for access to information of this sort; that is, information stored in electronic mail systems.

Mr. **Moorhead**. I think from the public's point of view the biggest problem that they see is with these cellular phones. People are selling devices that they advertise can scan the airwaves to pick up cellular telephone conversations. People can hear all kinds of gossip that is of no business to them or even pick up information that can be useful in the financial world and elsewhere. Maybe you can stop the sale of these devices or force them to make them such that they cannot be used to get this particular area of the spectrum where cellular calls are coming in. But I wonder how you are ever going to stop the public that have those devices from using them. It would be very, very difficult——

Mr. **Walker**. Well, Mr. Moorhead, following me is a witness from the cellular communications industry, and I think I would prefer to let him respond to that question in terms of the particulars as it relates to cellular. I would only say again with reference to the electronic mail industry fortunately for us there seems to be no counterpart. You can't scan the airwaves, if you will, and intercept electronic mail in the same fashion. What you can do is sit down at your personal computer and access a system somewhere and try to devise a method of cracking the security safeguards on that system, and penetrate the system and then access information in the computer's files.

And this, frankly, doesn't have to be electronic messages. It could be data files. It could be any information stored in that computer. That has become a serious problem across the country, and our industry is quite concerned about it, as I think you will find the computer service industry generally is concerned.

Mr. **Moorhead**. Thank you very much.

Mr. **Kastenmeier**. One last question which is really a followup of my colleague's question. Do I understand the present practice with respect to governmental investigative agencies, either for criminal or intelligence purposes, in obtaining copies of messages sent by electronic mail has been for them to get a court order, or is that somewhat in the murky area, too?

Mr. **Walker**. Well, again I am only aware of one instance that has been reported. In that case, the Government obtained a subpoena I am told.

Mr. **Kastenmeier**. The Government subpoenaed——

Mr. **Walker**. The document.

Mr. **Kastenmeier** [continuing]. Rather than obtain a warrant as they would under——

Mr. **Walker**. That's my understanding; yes. But I can't say that represents a general pattern. I don't know that you can generalize from one instance.

Mr. **Kastenmeier**. I think in my experience, having been through the late 1960's, that there was a period of time in which telephone companies, banks, and others chose not to cooperate sub rosa with Government agencies. They found themselves very vulnerable in terms of customer relationships and the law because people started to litigate these questions. So, it gave rise to broad support for clear governmental procedures under which records held privately could be released to the Government; that is, under warrants or other court orders. That seems again to be the case today. There is a corollary in which there is some uncertainty in the role of communications service providers with respect to Government agencies, either for criminal or intelligence purposes.

Mr. **Walker**. That is right. As providers of electronic mail services, we feel it is very important to that we protect the privacy of our customers to the utmost, and not release any information that we may have available in our computers. Yet we, on the other hand, feel there are legitimate law enforcement objectives that need to be served, and it would put the service provider in a very difficult position if a request were made for information and there was no clear standard as to whether that information should be released.

So, the bill in providing that guidance I think will set at ease the minds not only of the service providers, but also the users.

Mr. **Kastenmeier**. According to a recent Office of Technology Assessment study, there are at least six Government agencies that resort to interception of electronic mail. So, as you say, we certainly have to clarify the situation.

I have no further questions. I want to thank you very much, Mr. Walker and Mr. Cavanagh, not only for your testimony here today, but for the work that you have done preceding this in working with the Congress in this important area, and also to say to you that we doubtless will have to talk to you again, perhaps at some length, as legislation goes through the route and we developed a better understanding of some of the subtle impacts the legislation may have, not only on your industry, but generally.

In any event, thank you very much.

Mr. **Walker**. Thank you, Mr. Chairman. We look forward to continuing that dialog.

Mr. KASTENMEIER. Our next and last witness for this morning is Mr. Philip J. Quigley, president and chief executive officer of PacTel Mobile Co.'s of Costa Mesa, CA. PacTel is the Nation's largest cellular telephone company with 35,000 customers. Mr. Quigley has been in the telecommunications industry since 1967, when he started with Pacific Telephone.

Mr. Quigley, we are delighted to welcome you here this morning. We have your statement, and you may proceed from it if you wish, or however you care to. We are happy to have you.

## TESTIMONY OF PHILIP J. QUIGLEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, PACTEL MOBILE CO.'S, ACCOMPANIED BY ROBERT W. MAHER, EXECUTIVE DIRECTOR, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Mr. QUIGLEY. Good morning, Mr. Chairman, and members of the subcommittee. I would like to take this opportunity to thank you for allowing us to testify today in support of H.R. 3378, the Electronic Communications Privacy Act of 1985, and particularly commend the chairman and my fellow Californian, Congressman Moorhead, for their sponsorship of this very important bill.

I have with me today, Bob Maher, who is the executive director of the Cellular Telecommunications Industry Association. That is the group and the members of which I represent today. As I am sure you know, cellular telecommunications is an advanced form of mobile telephone service that weds computer technology with radio spectrum into a highly efficient and reliable communications tool for people who conduct business out of their office and are generally on the move. CTIA represents all segments of the industry, including both wireline and nonwireline carriers, resellers of cellular service, and also manufacturers of cellular equipment. Our association represents almost 90 percent of the cellular operators operating in the United States.

Let me begin by saying the right of privacy is a fundamental personal right. Many times, under varied circumstances, the Supreme Court has upheld this right, finding that it emanated "from the totality of the constitutional scheme under which we live." As Justice Brandeis explained more than 50 years ago, privacy is "the most comprehensive of rights and the right most valued by civilized men."

It has often been noted that the development of electronic communications has brought the people of our Nation and the world closer together, and has served to create new business and personal relationships and to enhance old ones. With these benefits, unfortunately, the development of electronic communications has also provided unscrupulous individuals with the opportunity to intrude upon the privacy of a conversation through the use of wiretaps or radio receiving devices.

The authors of the 1968 wiretap law sought "to prevent or deter improper invasions of privacy," in part by protecting telephone conversations against interception. However, the law equated telephone conversations with wire communications. As technology has developed to transmit telephone conversations over radio frequencies as is the case with cellular, rather than through wires or cables, the applicability of the 1968 act has become increasingly unclear and murky.

In effect, technology has leapfrogged the law. We are pleased with H.R. 3378 and today's proceedings because they are, we hope, witness that Congress is moving to reassert the original intent of the 1968 act, safeguarding the fundamental right of our citizens to privacy.

The issue of nonwire telephony goes beyond cellular communications. Even calls made over conventional telephones today in the home or office may be transmitted only in part over wires. For much of the distance they travel, such calls are often transmitted by radio in the form of terrestrial microwave or satellite. Because these calls are transmitted over both wire and radio, there is some question as to the applicability of the privacy law. If, for example, a call is intercepted on the radio leg of a transmission rather than on the wire leg, the law may offer little or no privacy protection.

Almost since the Privacy Act was passed, courts have had to consider whether and to what extent the statute applies to the communications transmitted in part by wire and in part by radio. The results have been mixed. In 1970, for instance, one Federal court held there was no reasonable expectation of privacy for calls transmitted over a mobile car telephone when the conversations could be easily overheard with an FM radio receiver. Three years later, another Federal court concluded that the statute offered no privacy protection to calls placed from one radio-telephone to another, but that radio-telephone conversations were protected if they traversed a conventional telephone network.

More recently, a number of State courts have addressed the vesting question of applying the 1968 act to conversations over mobile and cordless telephones. These courts concluded that conversations transmitted over the radio spectrum are neither wire communication, because they are transmitted at least in part by radio, nor oral communication, because a person communicating by radio has no reasonable expectation of privacy, and so fall outside the scope of the current Privacy Act regardless of whether they traverse the conventional wired telephone network.

While none of these cases involved cellular service, their inconsistent approach to the law cast a shadow of uncertainty over the privacy rights of all users of mobile communications. It is incumbent upon Congress to make explicit that the law is not technology specific, but guarantees the privacy of all electronic communications. CTIA feels very strongly that advances in communications technology should in no way diminish the right of privacy. To the contrary, the right of privacy must be protected especially in the face of technological change.

Today, for instance, after 13 years of regulatory delay at the FCC, cellular communications systems are up and operating in 80 markets throughout the United States, and cellular is riding a steep growth curve. It is anticipated that within 5 years there will be almost 2 million subscribers of cellular service, and industry will equate to approximately $2 billion in revenue.

I mentioned in the opening that we are in the process of building, continuing to build one of the largest systems in the world. Currently, in Los Angeles we have almost 35,000 subscribers that not only use their service in Los Angeles, but also in San Diego and Sacramento and, as I did yesterday as I came from California, stopping in Houston, while I was still on the plane used this portable telephone to call my office to see what was in abeyance, what action was required since I had left the office.

These portable phones are going to become more and more common and I am sure, Congressman, as you leave Washington to meet with your own constituency you find that you have a need to communicate back with the office or forward to your next destination. This kind of portable technology is not the thing of the future, it is really today's technology. And I submit that you, as other business people throughout the country today, will have a continuing need to move ahead with this new technology and experience its benefits of productivity.

The substantial demand for high-quality, mobile communications is not surprising. Again, a need to keep in touch with efficient communications; that works when you want it to work.

However, the growth of cellular and its contribution to economic development are closely tied to the legislation before this subcommittee today. Users of sophisticated communications services like cellular have a reasonable expectation of privacy when they pick up the phone, as they should. Without the certainty of legislation, however, the task of defending the right could take years of litigation in the courts.

For these reasons, CTIA supports H.R. 3378. This bill would remove the cloud over the privacy rights of cellular communications by revising the privacy statute to replace wire communications with electronic communications, the willful interception of which would be prohibited under the criminal code. The Electronic Communications Privacy Act of 1985 will bring the historic American guarantee of privacy protection into the information age. By protecting the security of conversations regardless of the medium of transmission, the legislation will encourage the continued growth and development of new and more effective means of communication, including cellular communications.

Of course, even if H.R. 3378 is enacted, there will still be some people who flout the law and intentionally listen in on private conversations transmitted via the radio spectrum. Individuals can use scanning devices today. And it is not our intent to impose any restrictions on the common public channels that are available for scanning today, but frankly to merely excise out of those scanning capabilities the capability that exists today to zone in on the channels and the frequencies that are associated with cellular telephony.

One way to close this loophole would be to limit the frequencies again that scanners can receive. We have had discussions with the FCC, and it is very unclear as to what their position is. I am certain that this legislation will have a serious impact on influencing their view of what might be done to control scanning devices.

Again, I would like to thank the subcommittee for their action in sponsoring this bill and inviting us to appear today, and at this point I would be happy to answer any questions.

[The statement of Mr. Quigley follows:]

CTIA

STATEMENT OF PHILIP J. QUIGLEY
PRESIDENT AND CHIEF EXECUTIVE OFFICER, PACTEL MOBILE COMPANIES

BEFORE THE SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE

ON

H.R. 3378, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985

SEPTEMBER 26, 1985

Mr. Chairman, Members of the Subcommittee:

My name is Philip J. Quigley. I am the President and Chief Executive Officer of PacTel Mobile Companies, whose subsidiary, PacTel Mobile Access, provides cellular communications services in California. Thank you for the opportunity to testify this morning in support of H.R. 3378, the Electronic Communications Privacy Act of 1985.

I am appearing before you today on behalf of the Cellular Telecommunications Industry Association. Cellular communications is an advanced form of mobile telephone service that weds computer technology and the radio spectrum into a highly efficient and reliable communications tool for people who conduct business out of the office, and for others in our society who find themselves increasingly away from home. CTIA represents all segments of the cellular industry, including both "wireline" carriers -- cellular carriers affiliated with conventional local telephone companies -- and "non-wireline" carriers; resellers of cellular service; and manufacturers of cellular equipment. CTIA's members represent almost 90 percent of all cellular operators.

The right of privacy is a fundamental personal right. Many times, under varied circumstances, the Supreme Court has upheld this right, finding that it emanated "from the totality of the constitutional scheme under which we live."[1] As Justice Brandeis explained more than 50 years ago, privacy is "the most comprehensive of rights and the right most valued by civilized men."[1]

It has often been noted that the development of electronic communications has brought the people of our nation and the world closer together, and has served to create new business and personal relationships and to enhance old ones. With these benefits, unfortunately, the development of electronic communications has also provided unscrupulous individuals with the opportunity to intrude upon the privacy of a conversation through the use of wiretaps or radio receiving devices.

The authors of the 1968 wiretap law sought "to prevent or deter improper invasions of privacy,"[1] in part by protecting telephone conversations against interception. However, the law equated "telephone conversations" with "wire communications." As technology has developed to transmit telephone conversations over radio frequencies rather than through wires or cables, the applicability of the 1968 act has become increasingly unclear.

---

[1] Poe v. Ullman, 367 U.S. 497, 517 (Douglas, J., dissenting).

[1] Olmstead v. United States, 277 U.S. 438, 478 (1927)(Brandeis, J., dissenting).

[1] Zweibon v. Mitchell, 606 F.2d 1172, 1182 (D.C.Cir. 1979), cert. denied, 453 U.S. 912 (1981).

In effect, technology has leapfrogged the law. We are pleased with H.R. 3378 and today's proceedings because they are, we hope, witness that Congress is moving to reassert the original intent of the 1968 act -- safeguarding the fundamental right of our citizens to privacy.

The issue of "non-wire" telephony goes beyond cellular communications. Even calls made over "conventional" telephones in the home or office may be transmitted only in part over wires. For much of the distance they travel, such calls are often transmitted by radio in the form of terrestrial microwave or satellite. Because these calls are transmitted over both wire and radio, there is some question as to the applicability of the privacy law. If, for example, a call is intercepted on the "radio" leg of the transmission rather than on the "wire" leg, the law may offer little or no privacy protection.

Almost since the privacy act was passed, courts have had to consider whether and to what extent the statute applies to communications transmitted in part by wire and in part by radio. The results have been mixed. In 1970, for instance, one Federal court held that there was no reasonable expectation of privacy for calls transmitted over a mobile car telephone when the conversations could easily be overheard with an FM radio receiver.[4] Three years later, another Federal court concluded that the statute offered no privacy protection to calls placed from one radio-telephone to another, but that radio-telephone conversations were protected if they traversed a conventional telephone network.[5]

More recently, a number of state courts have addressed the vexing question of applying the 1968 act to conversations over mobile and cordless telephones. Those courts concluded that conversations transmitted over the radio spectrum are neither wire communication (because they are transmitted, at least in part, by radio) nor oral communication (because a person communicating by radio has no reasonable expectation of privacy), and so fall outside the scope of the current privacy act regardless of whether they traverse the conventional wired telephone network.[6]

While none of these cases involved cellular service, their inconsistent approaches to the law cast a shadow of uncertainty over the privacy rights of all users of mobile communications. It is incumbent upon Congress to make explicit that the law is not technology-specific, but guarantees the privacy of *all* electronic communications. CTIA feels strongly that advances in communications technology should in no way diminish the right of privacy. To the contrary, the right of privacy must be protected especially in the face of technological change.[1]

---

[4] United States v. Hoffa, 436 F.2d 1243 (7th Cir. 1970), cert. denied, 400 U.S. 1000 (1971).

[5] United States v. Hall, 488 F.2d 193 (9th Cir. 1973).

[6] Rhode Island v. Delaurier, 488 A.2d 688 (R.I. 1985); Kansas v. Howard, 679 P.2d 197 (Kans. 1984); Dorsey v. Florida, 402 So.2d 1178 (Fla. 1981).

Today, for instance, after 13 years of regulatory delay at the FCC, cellular communications systems are up and operating in 80 markets throughout the United States -- and cellular is riding a steep growth curve. Within five years, there will be almost two million subscribers of cellular service, including not only the now-familiar car telephones but also portable "pocket phones" like those demonstrated last week at an industry trade show.

The substantial demand for high-quality mobile communications is not surprising, given the increasing mobility of American society and the constant need for many, particularly in business, to "keep in touch" with the office, customers, or clients. Moreover, the more efficient communications made possible by the cellular industry will enhance the productivity and competitive edge of American business.

---

[1] *See, e.g.*, *Olmstead v. United States*, 277 U.S. 438, 473-4 (Brandeis, J., dissenting); *Silverman v. United States*, 365 U.S. 505, 508-12.

However, the growth of cellular -- and its contribution to economic development -- are closely tied to the legislation before this Subcommittee today. Users of a sophisticated communications service like cellular have a reasonable expectation of privacy when they pick up the phone -- as they should. Without the certainty of legislation, however, the task of defending that right could take years of litigation in the courts.

For these reasons, CTIA supports H.R. 3378. H.R. 3378 would remove the cloud over the privacy rights of cellular communications by revising the privacy statute to replace "wire communication" with "electronic communication," the willful interception of which would be prohibited under the criminal code.[1] The Electronic Communications Privacy Act of 1985 will bring the historic American guarantee of privacy protection into the Information Age. By protecting the security of conversations regardless of the medium of transmission, the legislation will encourage the continued growth and development of new and more effective means of communication, including cellular communications.

---

[1] "Electronic communication" is defined as "any transmission of signs, signals, writing, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic or photoelectric system that affects interstate or foreign commerce." H.R. _____, 99th Cong., 1st Sess., § 101(a)(1) (1985).

Of course, even if H.R. 3378 is enacted, there will still be some people who will flout the law and intentionally listen in on private conversations transmitted via the radio spectrum. Today, these people can use scanning receivers -- popularly known as "scanners" -- to eavesdrop on cellular conversations, because scanners are engineered to receive not only communications readily available to the public (such as police and fire communications) but also communications in the frequency bands reserved for cellular.

One way to close this loophole would be to limit the frequencies that scanners can receive. CTIA is not interested in preventing any person from intercepting "public" communications such as police or fire calls, and we endorse the provisions in the pending legislation that exempt such communications from the privacy law. However, there is no reason why scanning equipment should be designed to receive frequencies that have been reserved for private communications. CTIA believes that an appropriate technical modification in the FCC's rules governing scanners is a necessary adjunct to the privacy legislation being considered by this Subcommittee.

We believe that the FCC currently has the authority to make such a modification. We are hopeful that the Congressional interest in privacy will make the agency more responsive to the problem than it has been in the past.

Again, I would like to thank the Subcommittee for inviting me today. I would be happy to answer any questions you may have.

- / -

Mr. **Kastenmeier**. Thank you very much, Mr. Quigley. I am certainly impressed by your industry, what it has already achieved and its potential. I have two or three questions, but I would like to first yield to my colleague from California, Mr. Moorhead, a sponsor of the bill.

Mr. **Moorhead**. Thank you, and welcome back here to Washington from Costa Mesa.

I understand that the 800 frequency is the one that is basically used by the cellular phones. These scanners that are sold are such that you can tune in on that particular frequency and find out who is talking and what might be interesting that they could pick up; is that right?

Mr. **Quigley**. That is correct.

Mr. **Moorhead**. Is there any other purpose for that particular frequency besides the cellular phones?

Mr. **Quigley**. No; that frequency bandwidth is dedicated entirely to cellular. And it is not the entire 800-megahertz frequency but only portions of it which are dedicated solely to cellular.

Mr. **Moorhead**. Would it be possible to forbid the use of that particular frequency to these scanners? Would there be any legitimate purpose that would be thwarted if you did that?

Mr. **Quigley**. Yes, it is possible. While I am not representing the manufacturers in terms of their technical capability today, it is my understanding that it is possible to restrict the scanning capability to only those frequencies that might be allowed by law. And as a consequence, those that are involved in the private communications sense, such as cellular, where, by the way, Congressman Moorhead, approximately 85 percent of the calls that are made over cellular phones are to landline or received from landline customers. And that certainly they have the same expectation of privacy that landline customers have today, and that what you are suggesting is technically feasible; however, the scanners that are on the market today do allow that random access of that frequency band.

Mr. **Moorhead**. I know this has become a major issue in some of the media in southern California and they have gone out themselves to see what they can listen to, to try to discover how many people are eavesdropping on others, and so forth. There has even been editorials about the subject.

Do you feel that this legislation that we are working on now will take care of the problem?

Mr. **Quigley**. Just a comment on your comments on the editorial coverage in southern California. Let me quote from one of the excerpts of KNX Radio, from one of the reporters. He says: "These devices monitor random phone calls and only within a limited radius. But as I found out, you can hear entire conversations from beginning to end, one right after another. These are very private conversations between attorneys and clients, husbands and wives, movie stars and their agents."

Our analysis of your bill, Congressman, will do exactly what you propose it will do. No. 1, it will set that standard of privacy that people expect and will encourage other agencies to respond to the need to restrict devices to only those frequencies that one should be allowed to hear conversations on. And that once that bill is enacted the momentum will have gained. The individuals in the industry will understand the protections of the law. And when I am before the press, as I am often, I can respond as I have recently after the passage of the bill in California on privacy, recently signed by Governor Deukmejian, that in fact, yes, it is illegal to intercept and misuse private conversations.

Mr. MOORHEAD. One question that has to come up: How can you stop the folks who already have scanners from using them just to satisfy their curiosity about other people's affairs and their business?

Mr. QUIGLEY. Well, I think practically speaking it would be difficult to recall scanners that have been sold on the market. But certainly a signal would be sent if there was a restriction on manufacturers proliferating those scanners. Again, I think maybe this is a bizarre analogy, but the fact of the matter is there are a lot of handguns on the market today and a few of them are misused. And again, if a standard is established and if the law is understood, then, hopefully, people will abide by that law.

Mr. MOORHEAD. Thank you.

Mr. KASTENMEIER. One thing the bill does not precisely define is "electronic communication providers." I raised this question before. Do you think the bill should or should not be amended to provide a much more specific definition of a "service provider" or should we encourage the FCC to define the term?

Mr. QUIGLEY. It is our view that the definitional issue is best handled in Congress and should be very specific. Now one thing that one would observe in the previous Privacy Act is that it limited its applicability. It appears that this bill does not, that it does cover the pervasive issues associated with today's electronic issues as well as in the future.

Mr. KASTENMEIER. What relationship would you see to law enforcement or other legitimate governmental purposes? If the casual person, through a scanner, is able to intercept calls—even though we take pains in this legislation to proscribe that activity—should we also insist that the Government in order to overhear such calls obtain specific authority through warrants or other means such as in wiretapping?

Mr. QUIGLEY. Yes; we believe the same principles would apply. And in fact, today, just in our normal course of business we respond to various agencies for information; not of a scanning type, but of conversations or people who are customers of ours and their usage information. We do require that information by law, and I think that bill would protect that right also.

Mr. KASTENMEIER. Would it not be the case that it would be an advantage to your industry? Your industry would be able to be more attractive, in terms of customers, if the public thought that calls being made were in fact protected by privacy, either from a technological standpoint or from a law standpoint, rather than easily intercepted?

Mr. QUIGLEY. As a matter of fact, Mr. Chairman, that expectation exists today with our customers. I have been asked by prospective major account customers as to the privacy aspects of this technology. There is no question that the expectation is there today, that the industry will benefit, proliferate with further assurances of privacy.

One of the questions that I often received, or one of the responses that I get when I ask the question about the technological aspects that could ensure privacy are as follows: I met with Motorola the day before yesterday and we talked about the issue of privacy and from a public policy standpoint how it should be addressed versus a technology standpoint. And there is no encryption solution today or in the near term that would assist privacy. And when it comes about, which is estimated probably in about 5 years, it would probably cost an individual about $500 to ensure privacy of his or her conversations.

There is no doubt in my mind that it is a basic underlying expectation of the public. There is no question that most of the conversations are to landline customers or over landline facilities, in addition to radio facilities, and, in fact, this business would benefit by the provisions contained in this bill.

Mr. **Kastenmeier**. We don't want to get too technical, but one of the assumptions is that before seeking legal protection through such a bill or law as this that the electronic communication provider itself take steps to prevent easy interception before relying on government. In that connection, noting that it would be difficult, what steps have the cellular phone companies actually taken to protect the privacy of the calls made over your phones?

Mr. **Quigley**. Well, our fundamental principle that we have been operating on is that it is a basic constitutional right to privacy that everybody has. Again, from a technology standpoint, internally we assure our customers that their conversations are not going to be used or observed in any way to disadvantage them. Strictly from an internal and an operational standpoint we protect their rights to privacy. Unfortunately, because airwaves are airwaves it is very difficult to come up with a technological solution to protect them to the degree we would like to.

We have had ongoing conversations with manufacturers in the industry, and it is a very, very difficult technological challenge, again, to ensure the right to privacy through encryption devices. It is down the road, it is going to be a very costly alternative and, again, that is why we feel that the basic right being a constitutional one should be preserved.

Mr. **Kastenmeier**. Of course at the present time I take it you are exclusively in aural communications. Is there any possibility that you will go to video as well as aural at some point in time?

Mr. **Quigley**. There are data applications currently being used, and there is no question that while they are not available today that textual matter and video could be the next stage of evolution in cellular technology. It is not impossible at all. No. 1, it is an issue of market; and, second, whether or not the cost will bear up under the market demand.

Mr. **Kastenmeier**. From your perspective, as one who has looked at this bill and supports it, do you think it sufficiently anticipates technology and problems relating to privacy?

Mr. **Quigley**. Our view is it does, Mr. Chairman, in that it becomes by definition a reference to the evolving electronic solutions that will come out to the transfer of voice and data, as you say, and other types of displayed information. It appears to meet that test to us; yes.

Mr. **Kastenmeier.** Mr. Quigley, we appreciate your testimony here this morning. It has been very helpful. Obviously, your industry is one that plays a central role in terms of the need and use of such legislation. We appreciate that.

In any event, as with the prior witness, we also may need to be in touch with you and your industry before we conclude legislative processing of this bill, but we appreciate the contribution you have already made in this area. Thank you very much.

Mr. **Quigley.** Thank you, Mr. Chairman. Again, we commend you and members of the subcommittee for drafting this very important bill. I think it is an enlightened attempt and will result in exactly what we feel is necessary in the telecommunications marketplace.

Mr. **Kastenmeier.** This concludes the hearing today, the first hearing on the question of communications privacy legislation. A subsequent hearing date will be announced shortly.

[Whereupon, at 11:32 a.m., the subcommittee was adjourned, to reconvene subject to the call of the Chair.]

# ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

THURSDAY, OCTOBER 24, 1985

House of Representatives,
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice,
Committee on the Judiciary,
*Washington, DC.*

The subcommittee met, pursuant to adjournment, at 10:15 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier, Boucher, Schroeder, Kindness, Berman, Moorhead, Coble, and Swindall.

Staff present: Deborah Leavy and David Beier, counsel; Joseph V. Wolfe, associate counsel; and Audrey Marcus, clerk.

Mr. Kastenmeier. The committee will come to order.

Without objection, the committee will permit the meeting this morning to be covered in whole or in part by television broadcast, radio broadcast, and/or still photography, pursuant to rule V of the committee rules.

This morning the subcommittee is holding its second day of hearings on H.R. 3378, the Electronic Communications Privacy Act of 1985. I'm also pleased to release a study by the Office of Technology Assessment [OTA], on electronic surveillance and civil liberties. This study, responding to a request I made 2 years ago, is an expert, nonpartisan examination of new communications technologies and the privacy protection that is afforded under current law. This study identifies problem areas and provides Congress with the intellectual groundwork for legislative solutions.

During our hearing today, we will receive testimony from the OTA summarizing this important work. The subcommittee will also hear from representatives of two trade associations, ADAPSO and Telocator.

The subcommittee appreciates the strong showing of interest in this legislation. We expect to conduct one, possibly two more hearings on the bill this year, and move to markup perhaps not this year but, certainly, early next year. Meanwhile, the subcommittee staff will be meeting with representatives of the Department of Justice, the FCC, and various trade and industry associations in an effort to clear the way and suggest how we might resolve minor drafting issues. It is my intention either to print a series of these amendments in the Congressional Record, or, with the cooperation of my colleagues, to reintroduce a clean bill prior to markup.

Now I would like to greet as our first witness this morning Mr. Fred W. Weingarten, Program Manager for the Communications and Informations Technologies Program of the Office of Technology Assessment. Mr. Weingarten came to the OTA in 1980 from the National Science Foundation, where he developed the first program support for computer science research. Mr. Weingarten has been very helpful to this subcommittee on a number of occasions as a witness, as director of this study and on another study on copyright and technological change which, I understand, will be forthcoming shortly.

Mr. Weingarten, I would like to welcome you here this morning. We have your statement and you may proceed as you wish.

## TESTIMONY OF FRED W. WEINGARTEN, PROGRAM MANAGER, COMMUNICATION AND TECHNOLOGIES PROGRAM, OFFICE OF TECHNOLOGY ASSESSMENT

**Mr. WEINGARTEN.** Yes, sir. Thank you very much, Mr. Chairman.

**Mr. KASTENMEIER.** We will receive, make part of the record, the report you tender, together with your statement and the appendixes to it. You may summarize your statement if you wish.

**Mr. WEINGARTEN.** Thank you very much, sir. It certainly is a pleasure to be here on a dual occasion for us: One, to participate in the hearings on your bill, H.R. 3378; and second, to participate in your release of our report, "Electronic Surveillance and Civil Liberties."

Before I comment on that report, I would like to acknowledge a couple of people who worked very hard on that. I sometimes feel guilty in being the representative of work that is done by other people in my program.

Dr. Fred Wood, behind me, is the project director of the larger project on Government information technologies in which this particular piece of work was done. And Dr. Priscilla Regan, seated next to Dr. Wood, was the principal author of this specific study. If at a later time we get into discussions specifically addressing the content of the study, I might ask them to answer some of the questions of the committee.

**Mr. KASTENMEIER.** That would be fine. I certainly want to ask members of this committee and others interested to avail themselves of this 72-page report. It took about 2 years to compile. But I am well aware of how difficult it is if you are monitoring a number of different Federal agencies to determine what their practices are, over a period of time. It takes a long time.

**Mr. WEINGARTEN.** Yes, sir, and this is also part of a much broader comprehensive look that we're doing at that study; that is, addressing other issues of civil liberties and management and administration of Government information practices. More parts of that will be released over the next few months.

The most fundamental summary I could make of my testimony and of this report is that the telecommunications infrastructure in this country is undergoing a revolution. That word is used very often these days, with a number of technologies. In this case, it is used quite accurately. The revolution has been taking place over the past decade or two, and probably will continue to take place through the foreseeable future.

To illustrate, I would like to refer to two figures that appear in the back of my written testimony. Figure 1 represents the metaphor, or model, of the telecommunications network that was used for the original consideration of wiretapping legislation about 17 years ago. Figure 2 is my attempt to sketch what the communications network of today and tomorrow is turning into.

Because of time demands and the schedule date of this hearing, at some point I had to stop developing that figure. Day by day I added new services, new connections, and new technologies to it. It is still a very incomplete figure. The point of it is, however, that the information infrastructure in this country is exceptionally complex and growing more complex, and any legislation that attempts to address that infrastructure, provide a road map, rules of the road, so to speak——

Mr. KASTENMEIER. Mr. Weingarten, if I could just interrupt. For visual purposes, I'm going to hold up the report, since the impact is lost without seeing it. It's too bad we don't have a large chart.

Here you have a phone, copper wire, and then you're suggesting, that either by wire or by radio there's a further transmission to the copper wire and the phone at the other end. That was simply how telephone communications were regarded a decade or two ago. But now, you've suggested that technology has this very complex system of multiple ways of transmission through the new technology, and of the complex involvement of a number of systems.

I don't think it would pay for us to ask you to explain that, but let's just say the quantum of complexity and difficulty has grown enormously. Will the laws and statutes written in former days become inapplicable as they are increasingly out of touch with contemporary technology?

Mr. WEINGARTEN. Yes, sir. In fact, what happened was that an attempt to provide a simple illustration to my testimony ended up with the basic metaphor of our report and of this testimony—that the system itself was undergoing such an enormous, fundamental change that the Congress is confronted, with a variety of legislative problems.

A variety of new technologies is involved, from cellular telephones, to cordless telephones, to satellite transmission and fiber optic transmissions.

There is a variety of system operators. We are no longer dealing with a single monopoly provider of public communications, but a variety of operators competing in the marketplace. In many cases banks and other large organizations design, own, and operate their telecommunications systems. As individuals, we own far more of that network than we did in the past.

Finally, there's a variety and increasing value of information that is flowing through the network, from what used to be simple telephone conversations to stock market transactions, electronic mail, paging messages, and computer data of all kinds flowing through that network. The complexity of it is illustrated by the overall shape of the drawing, rather than the details of it.

One of the most important points that comes from figure 2 is that any attempt to try to define legislatively specific paths through this network, to call one path a "phone call," another path "electronic mail," another path "electronic funds transfer," is like trying to write with ink on flowing water. The nature of the services and the nature of the network is changing so rapidly, is in such a state of flux, that such attempts are bound to fail, to end up being ineffective almost before the legislation has been printed.

Lest this seem to be a very futuristic view, I'd like to bring in an example, without naming names, that I came across just yesterday. When in a local bank, I was handed a brochure describing a new investment service. A person could have their home computer connected through a telephone network to a bank computer that kept records on the investment portfolio and transactions of that person. That, in turn, was connected to a stock market quotation data base providing instant quotations on the price and volume, transactions on any stock. The user is also connected to a transaction system through which one could order the sale or a purchase of securities. This is an example of the variety of new services that are being developed on top of this network that seem to warrant protection. Much is unprotected, technologically and legally, in that kind of an application.

Furthermore, the value of the information is much greater to the owner. In past discussions about wiretapping, people would often say, "I don't care if anybody overhears my phone conversations. They're innocuous; there's nothing of value in them. It's usually my teenager talking to her friends." Now, it's investment decisions, it's financial information flowing from the home over that network to some computer.

The value of the information is greater not only to the owner or user of that network, but to somebody else from the outside who would like access, either for legitimate or illegitimate purposes. If I were a client, someone who could penetrate that system could purchase or sell securities in my name, or could get access to my financial information for a variety of purposes, including law enforcement.

There are two dangers in leaving this type of new application unprotected. One danger, of course, is a gradual erosion of privacy, a loss of the right to whisper and to keep our dealings confidential. The other danger is that we may be denied useful applications and useful new technologies because they're unprotected. Consumers and users simply will not use these services if they are not properly protected, and they will not be developed and offered in the marketplace.

Since we are entering what some people call an information age, in which our dependence on these new high technologies is increasingly profound. There is an important motivation for making sure that our laws and rules that regulate this technology are up to date and reflect the state of the technology.

In summary, OTA found, first that, due to the technological advance, protections previously accorded to certain forms of communication are being eroded and new applications and forms of communication are simply not covered under current law.

Second, in an information society, the stakes in providing such protections are ever higher.

Finally, if Congress wishes to restore these old protections and provide new ones, a comprehensive approach represented by, for instance, by bill H.R. 3378, may well be the only technologically feasible approach.

Mr. Chairman, I appreciate the opportunity to testify and will be glad to answer any questions.

[The statement of Mr. Weingarten follows:]

## TESTIMONY OF FRED W. WEINGARTEN
**PROGRAM MANAGER, COMMUNICATION AND TECHNOLOGIES PROGRAM**
**OFFICE OF TECHNOLOGY ASSESSMENT**
**U.S. CONGRESS**
**BEFORE THE HOUSE JUDICIARY SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,**
**AND ADMINISTRATION OF JUSTICE**
**OF THE HOUSE COMMITTEE ON THE JUDICIARY**

### ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES

October 24, 1985

Thank you Mr. Chairman. I am Fred W. Weingarten of the Office of Technology Assessment. I appreciate the opportunity to testify today on changing communication technologies as part of this Subcommittee's consideration of your bill H.R. 3378, the Electronic Communications Privacy Act of 1985.

I am also pleased on behalf of the Office of Technology Assessment that you are taking this occasion to release our new report, Electronic Surveillance and Civil Liberties. The report is part of a larger study of the effects of new information technologies on the Federal Government, which was requested by this subcommittee and by the Senate Committee on Government Affairs. We expect that the other pieces of that study will be completed in a few months.

In this study, we examined how new information technology is affecting the important issues of wiretapping and other forms of electronic surveillance, by providing new tools and opportunities that seem to be either not covered at all or ambiguously covered by current law. It is important to note, however, that we did not look specifically at technologies developed or used by national security agencies, nor did we examine policies concerning surveillance for national security purposes.

Our basic conclusion is as follows:

"The existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies."

In other words, technology, while providing the proverbial cornucopia of exciting new communications media and services, also seems to be in part responsible for chipping away inexorably at our personal privacy. It may be robbing us of our "right to whisper," to communicate in confidence. We have suggestive albeit incomplete evidence of the pervasiveness of electronic surveillance. For example, although our study revealed that little is known about the extent of electronic surveillance in the private sector, the responses to our Federal agency data request illustrate the scope of electronic surveillance on the part of the Federal Government and, as a result, suggest the importance of the issue to the Congress. In summary, we found that about 25% of the agency responses to our request indicated some use of electronic surveillance for law enforcement purposes and that its use is increasing. (Intelligence agencies were not included in the data request.)

This seems to be an area in which technology is rapidly outpacing law, and in which a carefully constructed historical balance between the need to maintain civil liberties and the need for government investigations has been upset. Your bill, H.R. 3378 addresses this issue.

Since our report provides a detailed analysis of the issues involved in surveillance legislation, I would like to spend my time before this subcommittee discussing in broader terms how technological change has presented us with these problems and the ways in which it creates stresses among the so-called "delicate balances" in our society.

## The Communications Revolution

We in the United States and, indeed, people all over the globe are experiencing a major revolution in how we communicate, why we communicate, and what we communicate. That revolution, which started a decade or two ago and will continue at least into the start of the next century, is driven by a combination of technological, institutional, economic, and social change.

Figures 1 and 2 represent graphically the change and illustrate why the term "revolution" is not an exaggeration, but is appropriately used to describe what is happening. Figure 1 represents the telecommunications system that held sway in this country for nearly a century. Although already starting to undergo a transformation, it was the model that was imbedded in the wiretapping provisions of the 1968 Omnibus Crime Control and Safe Streets Act. Figure 2 represents a partial view of the likely evolution of the telecommunications system of the future. Technology offers new media for communicating, as well as new tools for creating, storing, displaying and manipulating information. Deregulation and other forces in society are radically altering the structure of the industry that provides information and communication products and services. Computer-based automation in all sectors of industry increases the amount and value of information and information services to the health and competitiveness of our economy. Finally, the values, choices, and imaginations of individuals are shaping the demands for and the uses of information products and services -- from portable telephones to electronic bulletin boards and financial transactions.

The details of Figure 2 are not important. Many more services could be added to figure 2 and more connections could be illustrated. What is important are the characteristics of the new system that are illustrated, including:

- The variety of technological media used at various points.
- The incredible complexity of the system and the extent of interconnection.
- The variety of types of information all transmitted in the same forms over the same channels.
- The variety of institutions involved, from public common carriers, to specialized service providers, to individuals and firms that privately own portions of their communications sytems.

These characteristics greatly complicate the problems of striking an acceptable balance in electronic surveillance policy that will be robust over a reasonable length of time.

## Three Expectations

Although the underlying technology and uses of communication systems change, people seem to hold more constant expectations concerning their privacy and they may not be alert to a rapid change in the vulnerability of their communication to eavesdropping. These expectations are expressed in personal values and mores -- codes of behavior, as well as in law. (Secretary of State Henry L. Stimson, commenting on the interception by the U.S. Government of international message traffic, is reported to have stated, "Gentlemen do not read each other's mail." The Bill of Rights, particularly the Fourth Amendment, codifies some of those expectations as fundamental principles.)

In the debate over wiretapping and other forms of electronic surveillance, one comes frequently across the term "reasonable expectation of privacy." In asking how technology affects achieving the basic goals of public policy in this area, let us take the concept of "expectation" one step deeper in order to identify those goals. In particular, for analytical purposes we can identify three basic "expectations" that the public seems to have of Government in the area of surveillance.

1) The Right to Access: Individuals expect to have conveniently and publicly available channels of communication which they can enjoy with a reasonable level of privacy and protection from both private and unjustified government snooping. Public telephone service and first class mail are examples from the past of services protected by force of criminal law from unauthorized tampering. As we have seen, technological change, by removing certain traditionally protected channels of communication from protection, may deny people such access unless those protections are restored.

2) The Right to Knowledge: People have the right to know in advance what their protections and rights are in protected communications. One might expect those protections to be easily understood, consistent, and predictable. As our report states, technological change has thrown some law into a highly ambiguous state in which the level of protection is unknown and possibly considerably less than a citizen might expect. In some cases, (e.g., telephone calls) some protections afforded seem to depend on the particular technologies used, even though to most people these differences are incomprehensible and/or irrelevant.

3) The Right to Protection: Since the privacy of some communications

may serve broader societal as well as individual interests, a presumption rather than option of privacy is granted. These communications may not be optional and/or may contain potentially very sensitive information. For example, information communicated by a citizen to a Government agency such as the IRS or the Census Bureau are protected, as is the communication with a legal counsel, psychiatrist, or priest. New communication technology may offer new applications for which specific laws regarding privacy are needed. Congress has already had to act to specifically protect the privacy of cable television subscribers, for example.

Counterbalancing Considerations

Our society operates in a rough balance between openness and confidentiality. For most of this testimony, as well as in our report, we have focused on how new technology may be shifting that balance by eroding the privacy of personal life and communication. However, dangers could result from an overcorrection that shifts the balance too much in the other direction. Just as there are expectations of privacy, there are social interests in openess and in minimizing Federal control over human behavior. Let me mention a couple that have been raised in the course of our inquiry, both for this and other information policy studies.

- Criminalize Bad Manners: Not all instances of bad manners or unethical behavior are illegal. Behavior such as eavesdropping on private conversations and snooping into private papers by individuals is not totally covered by law. Instead, society regulates it through a less formal system of social rewards and punishments. As communications increasingly take electronic form and as laws and regulations are passed, such behavior may become subject to formal criminal rather than informal social sanction. Maybe in many cases it should be treated so, but we may need to build sufficient flexibility into the law to avoid criminalizing all bad manners.

o Decrease Social Accountability: The fact that communications are to some degree open, whether intentionally or through "leakiness," helps enforce public accountability for the behavior of people and organizations. Of course, we have already pointed out that the need for effective law enforcement is the most visible motivation for allowing controlled access to normally private communications, but such interests extend much further. For example, the investigative press, public interest groups, and even the Congress, itself, depend to some extent on open or leaky information flows to monitor for threats to the public interest in both the private and public sector. In this case, the danger may come from the accumulation of laws responding to the challenges of new information technology, covering issues ranging from intellectual property to wiretapping to computer crime. Each law may be well-founded, responsive to an important policy. (Certainly, we are not endorsing the right of anybody to wiretap, trespass, or break into computer data banks.) Yet, the net effect of the sum total of such laws could be to seal information, to create very large access barriers to the public.

## Effects of New Information Technology

The new communication and information technologies complicate efforts to regulate surveillance in several ways. Most of the problems arise from the fact that policy has traditionally, and quite naturally, varied depending on the characteristics of the particular technology and uses concerned. However, the natural result of this history has been to make the policies sensitive to technological change in several specific ways:

- Change in the Physical Medium: Some policies have assumed a particular technological model of communication. For example, the Omnibus Crime Control Act has been interpreted to cover voice telephone communications carried over a wire in analog form. Hence, as we point out in the report, the coverage of technologies such as digital transmission, cellular phones, cordless phones, electronic mail, and data communication in all forms is uncertain, at best.

- Change in Information Carried and Available: Traditionally, policy has concerned itself with the interception or recording of human conversations. As Figure 2 illustrates, the nature of data carried in a present or future system that provides information about an individual is much broader: electronic messages; personal notes and reminders, appointment calendars, and other information stored in an "automated desk-top;" video and facsimile data; and so on. Much of the data collected, stored, and transmitted by these new applications is not covered by current law.

- New Tools for Inferring Information: Powerful new computational techniques provide additional tools for deriving more information from the interception of even traditional communications. These include voice and image recognition technology, as well as speech understanding systems, and even, possibly in the future, techniques for inferring stress or emotional states. These technologies would increase the value, and hence, the potential sensitivity, of electronic eavesdropping.

- New Tools for Mass Surveillance: Surveillance, even in electronic form, has traditionally been labor intensive and expensive. Hence, it has been directed at specific individuals, and resource limitations have tended to be a disincentive for wide-scale use. Some new forms, such as video monitoring, may retain that characteristic. However, new computer technologies, such as image and speech understanding systems, can also provide improved economies of scale and essentially automate surveillance. For example, an increasing amount of information flows through certain identifiable central points in a communications network in digital form that is easily manipulated by computer. Hence, the ability to engage in mass surveillance may be greatly increased. The distinction between individual and mass surveillance has been crucial in assessing the civil liberties implications of surveillance.

- Less Detectable Monitoring: In some cases, technology change makes some forms of surveillance less detectable. Tapping the telephone copper wire "local loop" has been, by and large, detectable -- at least to technical experts. Other forms of surveillance, the television camera in the bank, the helicopter flying overhead, and so on are also highly visible, sometimes deliberately so. Some forms of modern surveillance technology are far less detectable, even by the operators of a communication network. Since policy has depended in part on the visibility of the surveillance this change may be important. Furthermore, to some, it also raises questions of enforcement and accountability.

- Inappropriate Models: The law, particularly as interpreted by the courts, often is based on identifying and applying historical analogies and definitions to new problems. But such analogies can be false and misleading in the new electronic world. For example, a glance at Figure 2 might lead one to wonder what will constitute a "telephone call" in the future when a single "call" may combine simultaneously or at various times such components as voice, video, facsimile, computer data, and financial transactions. Similar problems occur when we try to think about "electronic mail" as a form of mail or an "electronic bulletin board" as a form of bulletin board. Even traditionally useful concepts such as "public" and "private" become blurred in the electronic environment.

Summary

In sum, OTA found that new information and telecommunication technologies provide a potentially significant threat to the traditional privacy of communications and create new forms of surveillance that are not well covered by present law. The courts have requested guidelines from the Congress, and clarification of the rules would serve the needs of the criminal justice community as well as protect personal privacy. HR 3378 is an important effort at addressing the needs for legislative response.

It is a difficult area in which to legislate. Balances are difficult to achieve, and yet the desire for a robust law that will survive technological change is frustrated by the fast advance of electronics and the fertile imaginations of entrepreneurs who constantly dream up unexpected new ways to use that technology.

Mr. Chairman, again thank you for this opportunity to testify. I would be glad to answer any questions the subcommittee might have.

Figure 1.—The traditional telecommunication network

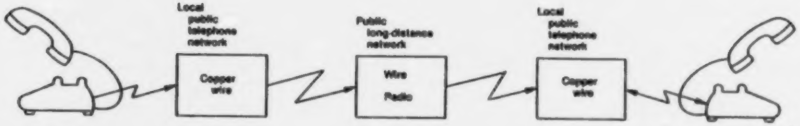
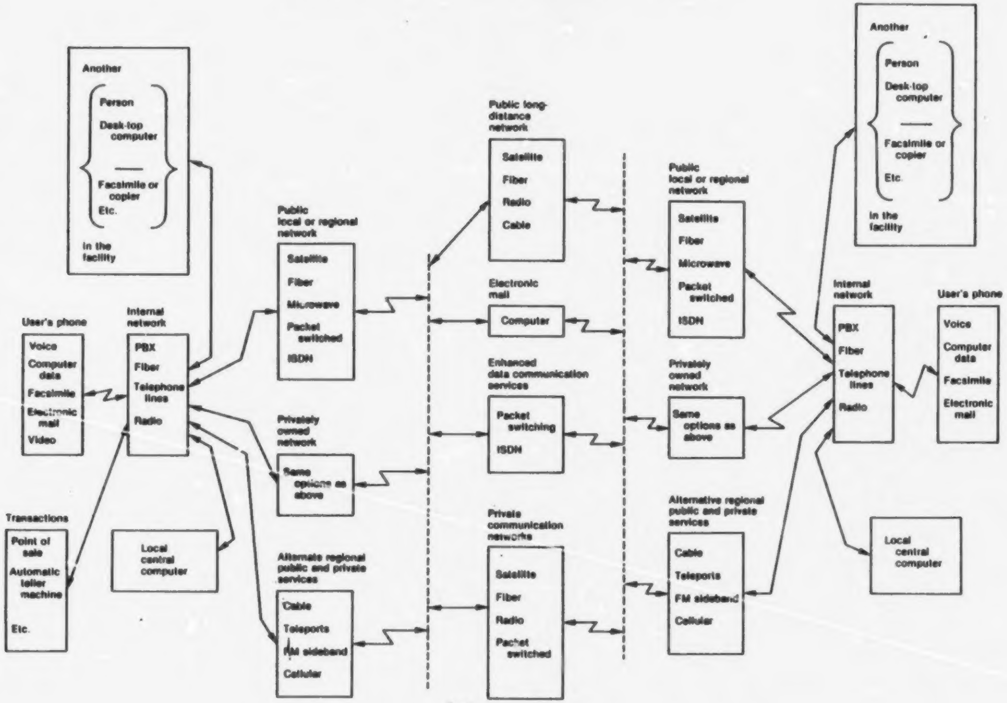

Local public telephone network
Copper wire
Public long-distance network
Wire
Radio
Local public telephone network
Copper wire

**Figure 2.—A View of the Future Telecommunications System**



58

## Federal Government Information Technology

# Electronic Surveillance and Civil Liberties

OTA Reports are the principal documentation of formal assessment projects. These projects are approved in advance by the Technology Assessment Board. At the conclusion of a project, the Board has the opportunity to review the report, but its release does not necessarily imply endorsement of the results by the Board or its individual members.

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D.C. 20510

# Foreword

Public policy on the use of information technology to electronically monitor individual movements, actions, and communications has been based on a careful balancing of the civil liberty versus law enforcement or investigative interests. New technologies—such as data transmission, electronic mail, cellular and cordless telephones, and miniature cameras—have outstripped the existing statutory framework for balancing these interests.

The primary technical focus of this report is on technological developments in the basic communication and information infrastructure of the United States that present new or changed opportunities for and vulnerabilities to electronic surveillance, not on the details of specific surveillance devices. The primary policy focus is on domestic law enforcement and investigative applications, not on foreign intelligence and counterintelligence applications.

Thus, this report addresses four major areas: 1) technological developments relevant to electronic surveillance; 2) current and prospective Federal agency use of surveillance technologies; 3) the interaction of technology and public law in the area of electronic surveillance, with special attention to the balancing of civil liberty and investigative interests; and 4) policy options that warrant congressional consideration, including the amendment of existing public law to eliminate gaps and ambiguities in current legal protections.

Conducted at the request of the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, and the Senate Committee on Governmental Affairs, this report is one component of the OTA assessment of "Federal Government Information Technology: Congressional Oversight and Civil Liberties." Other topics covered in the assessment include: information technology management, planning, procurement, and security; computer crime; computer matching and privacy; electronic dissemination of Government information; and computer-based decision support, modeling, and Government foresight. These will be published under separate cover.

In preparing this report on electronic surveillance, OTA has drawn on working papers developed by OTA staff and contractors, the comments of participants at an OTA workshop on this topic, and the results of an OTA Federal Agency Data Request that was completed by over 140 agency components. The draft of this report was reviewed by the OTA project advisory panel, officials from the U.S. Department of Justice, and a broad spectrum of interested individuals from the governmental, academic, private industry, and civil liberty communities.

OTA appreciates the participation of the advisory panelists, workshop participants, external reviewers, Federal agency officials, and others who helped bring this report to fruition. The report itself, however, is solely the responsibility of OTA, not of those who so ably advised and assisted us in its preparation.

John H. Gibbons

JOHN H. GIBBONS
*Director*

## Electronic Surveillance and Civil Liberties Advisory Panel

Theodore J. Lowi, *Chairman*
Professor of Political Science, Cornell University

Arthur G. Anderson
IBM Corp. (Ret.)

Jerry J. Berman
Legislative Counsel
American Civil Liberties Union

R. H. Bogumil
Past President
IEEE Society on Social Implications of Technology

James W. Carey
Dean, College of Communications
University of Illinois

Melvin Day
Vice President
Research Publications

Joseph W. Duncan
Corporate Economist
The Dun & Bradstreet Corp.

William H. Dutton
Associate Professor of Communications and Public Administration
Annenberg School of Communications
University of Southern California

David H. Flaherty
Professor of History and Law
University of Western Ontario

Carl Hammer
Sperry Corp. (Ret.)

Starr Roxanne Hiltz
Professor of Sociology
Upsala College

John C. Lautsch
Chairman, Computer Law Division
American Bar Association

Edward F. Madigan
Office of State Finance
State of Oklahoma

Marilyn Gell Mason
Director
Atlanta Public Library

William Joe Skinner
Corporate Vice President
Electronic Data Systems Corp.

Terril J. Steichen
President
New Perspectives Group, Ltd.

George B. Trubow
Director, Center for Information Technology and Privacy Law
The John Marshall Law School

Susan Welch
Professor and Chairperson
Department of Political Science
University of Nebraska

Alan F. Westin
Professor of Public Law and Government
Columbia University

Langdon Winner
Associate Professor of Political Science
Rensselaer Polytechnic Institute

### Congressional Agency Participants

Robert L. Chartrand
Senior Specialist
Congressional Research Service

Robert D. Harris
Deputy Assistant Director for Budget Analysis
Congressional Budget Office

Kenneth W. Hunter
Senior Associate Director for Program Information
U.S. General Accounting Office

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by these advisory panel members. The views expressed in this OTA report, however, are the sole responsibility of the Office of Technology Assessment.

## OTA Electronic Surveillance and Civil Liberties Project Staff

John Andelin, *Assistant Director, OTA*
*Science, Information, and Natural Resources Division*

Frederick W. Weingarten, *Communication and Information Technologies*
*Program Manager*

### Project Staff

Fred B. Wood, *Project Director*
Jean E. Smith, *Assistant Project Director*
Priscilla M. Regan, *Principal Author and Analyst*
Jim Dray, *Research Analyst*
Jennifer Nelson, *Research Assistant*

### Administrative Staff

Elizabeth A. Emanuel, *Administrative Assistant*
Shirley Gayheart, *Secretary*
Audrey Newman, *Secretary*
Renee Lloyd, *Secretary*
Patricia Keville, *Clerical Assistant*

### Contractor

Herman Schwartz, *The American University*

## OTA Electronic Surveillance and Civil Liberties Workshop

Stanley S. Arkin
Attorney

Peter Benitez
New York County District Attorney's
Office

Kier Boyd
Deputy Assistant Director
Technical Services Division
Federal Bureau of Investigation

James C. Carr
U.S. Magistrate

Floyd Clarke
Deputy Assistant Director
Criminal Division
Federal Bureau of Investigation

Russell Cestare
Chief of Liaison and Communication
Financial Investigations Division
U.S. Customs Service

Ronald C. Fann
Chief, Counterintelligence Operations
U.S. Department of the Army

Richard Gerstein
Partner
Bailey, Gerstein, Rashkind & Dresnick

Morton H. Halperin
Director
American Civil Liberties Union

Frederick D. Hess
Head, Office of Enforcement Operations
Criminal Division
U.S. Department of Justice

Mary Lawton
Counsel, Office of Intelligence and
Policy Review
U.S. Department of Justice

Frederick B. Lothrop
Analyst/Project Manager
PSC, Inc.

Paul Lyon
Chief of Special Operations
Bureau of Alcohol, Tobacco and Firearms
U.S. Department of the Treasury

Gary Marx
Professor, Department of Urban Studies
and Planning
Massachusetts Institute of Technology

Ronald S. Plesser
Attorney
Blum, Nash & Railsback

Christopher Pyle
Professor, Political Science Department
Mount Holyoke College

James B. Rule
Professor, Department of Sociology
State University of New York at
Stony Brook

Herman Schwartz
Professor of Law
The American University

L. Britt Snider
Director, Counterintelligence and
Security Policy
Office of the Secretary of Defense

**Other Reviewers**

Michael Cavanagh
Electronic Mail Association

Charles Miller
American Telephone & Telegraph Co.

David Peyton
Information Industry Association

Barbara Philips
Telocator Network of America

Harold Relyea
Congressional Research Service

# Contents

*Chapter* *Page*

1. **Summary** . . . . . . . . 3

2. **Introduction and Overview** . . . . . . . . 9
   - Summary . . . . . . . . 9
   - Introduction . . . . . . . . 11
   - Background . . . . . . . . 12
     - Technology and Use . . . . . . . . 12
     - Policy . . . . . . . . 15
   - Findings and Policy Implications . . . 21
   - Appendix 2A: Key Supreme Court Decisions on Electronic Surveillance . . . . . . . . 24
   - Appendix 2B: Key Statutes Relevant to Electronic Surveillance . . . . . . 25

3. **Telephone Surveillance** . . . . . . . . 29
   - Summary . . . . . . . . 29
   - Introduction . . . . . . . . 30
   - Background . . . . . . . . 31
   - Findings and Policy Implications . . . 34

4. **Electronic Mail Surveillance** . . . . . . . . 45
   - Summary . . . . . . . . 45
   - Introduction . . . . . . . . 45
   - Background . . . . . . . . 46
   - Findings and Policy Implications . . . 48

5. **Other Surveillance Issues** . . . . . . . . 55
   - Summary . . . . . . . . 55
     - Electronic Physical Surveillance . . . 55
     - Electronic Visual Surveillance . . . . . 55
     - Data Base Surveillance . . . . . . . . 56
   - Part I: Electronic Physical Surveillance . . . . . . . . 57
     - Introduction . . . . . . . . 57
     - Background . . . . . . . . 57
     - Findings and Policy Implications . . 59

*Chapter* *Page*

   - Part II: Electronic Visual Surveillance . . . . . . . . 62
     - Introduction . . . . . . . . 62
     - Background . . . . . . . . 63
     - Findings and Policy Implications . . 64
   - Part III: Data Base Surveillance . . . . 67
     - Introduction . . . . . . . . 67
     - Background . . . . . . . . 68
     - Findings and Policy Implications . . 70

## List of Tables

*Table No.* *Page*

1. Categories of Surveillance Technology . . . . . . . . 13
2. Categories of Behavior Subject to Electronic Surveillance . . . . . . . . 13
3. Top Fifteen Agency Components Using Electronic Surveillance Technology . . 14
4. Electronic Surveillance Technology: Current and Planned Agency Use . . . 15
5. Agency Components Indicating the Largest Projected Use of Electronic Surveillance Technology . . . . . . . . 15
6. Dimensions for Balancing Civil Liberty Interest v. Government Investigative Interest . . . . . . . . 22
7. Treasury Enforcement Communication System/Border Enforcement System Users . . . . . . . . 69
8. Source of Treasury Enforcement Communication System/Border Enforcement System Records . . . . . . . 69
9. Selected INS Computerized Record Systems . . . . . . . . 70

## Chapter 1

# Summary

In the last 20 years, there has been a virtual revolution in the technology relevant to electronic surveillance. Advances in electronics, semiconductors, computers, imaging, data bases, and related technologies have greatly increased the technical options for surveillance activities. Closed circuit television, electronic beepers and sensors, and advanced pen registers are being used to monitor many aspects of individual behavior. Additionally, new electronic technologies in use by individuals, such as cordless phones, electronic mail, and pagers, can be easily monitored for investigative, competitive, or personal reasons.

The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance applications. The fourth amendment—which protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures"—was written at a time when people conducted their affairs in a simple, direct, and personalized fashion. Telephones, credit cards, computers, and cameras did not exist. Although the principle of the fourth amendment is timeless, its application has not kept abreast of current technologies.

The major public law addressing electronic surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which was designed to protect the privacy of wire and oral communications. At the time Congress passed this act, electronic surveillance was limited primarily to simple telephone taps and concealed microphones (bugs). Since then, the basic communications infrastructure in the United States has been in rapid technological change. For example, satellite communication systems and digital switching and transmission technology are becoming pervasive, along with other easily intercepted technical applications such as cellular mobile radio, cordless telephones, electronic mail, computer conferencing, and electronic bulletin boards. Continued advances in computer-communications technology such as the Integrated Services Digital Network (ISDN), now close to implementation, are likely to present additional new opportunities for electronic surveillance.[1]

The law has not kept pace with these technological changes. The courts have, on several occasions, asked Congress to give guidance. Most recently, U.S. Circuit Court Judge Richard Posner, in a case involving the use of video surveillance in a law enforcement investigation, said:

> . . . we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope . . . judges are not authorized to amend statutes even to bring them up to date.

In legislating the appropriate uses of electronic surveillance, Congress attempts to strike a balance between civil liberties—especially those embodied in the first, fourth, and fifth amendments to the U.S. Constitution—and the needs of domestic law enforcement and investigative authorities for electronic surveillance in fighting crime, particularly white-collar and organized crime, and generally for drug, gambling, and racketeering investigations.[2]

Law enforcement and investigative agencies, at least at the Federal level, are making significant use of electronic surveillance techniques and are planning to use many new techniques. Based on a review of available reports and the results of its Federal Agency Data Request,[3] OTA found that:

---

[1] ISDN permits the transmission of voice, video, and data signals as needed over a common multi-purpose communications network.

[2] Note. This study did not review technology or policy issues concerning foreign intelligence and counterintelligence applications of electronic surveillance.

- The number of Federal court-approved bugs and wiretaps in 1984 was the highest ever.
- About 25 percent of Federal agency components responding (35 out of 142) indicated some current and/or planned use of various electronic surveillance technologies, including, but not limited to, the following:
  - —closed circuit television (29 agencies);
  - —night vision systems (22);
  - —miniature transmitters (21);
  - —electronic beepers and sensors (15);
  - —telephone taps, recorders, and pen registers (14);
  - —computer usage monitoring (6);
  - —electronic mail monitoring or interception (6);
  - —cellular radio interception (5);
  - —pattern recognition systems (4); and
  - —satellite interception (4).
- About 25 percent of Federal agency components responding (36 out of 142) report use of computerized record systems for law enforcement, investigative, or intelligence purposes:
  - —agencies reported a total of 85 computerized systems with, collectively, about 288 million records on 114 million persons;[4]
  - —examples of four such systems that could be used in part for data base surveillance purposes are the:
    1. National Crime Information Center (FBI),
    2. Treasury Enforcement Communications System (Treasury),
    3. Anti-Smuggling Information System (Immigration and Naturalization Service—INS), and
    4. National Automated Immigration Lookout System (INS).
  - —none of the 85 system operators provided the requested statistics on record quality (completeness and accuracy). Most do not maintain such statistics.

After conducting a review of the technology and policy history of electronic surveillance, OTA found that:

- The contents of phone conversations that are transmitted in digital form or calls made on cellular or cordless phones are not clearly protected by existing statutes.
- Data communications between computers and digital transmission of video and graphic images are not protected by existing statutes.
- There are several stages at which the contents of electronic mail messages could be intercepted: 1) at the terminal or in the electronic files of the sender, 2) while being communicated, 3) in the electronic mailbox of the receiver, 4) when printed into hardcopy, and 5) when retained in the files of the electronic mail company or provider for administrative purposes. Existing law offers little or no protection at most of these stages.
- Legislated policy on electronic physical surveillance (e.g., pagers and beepers) and electronic visual surveillance (e.g., closed circuit TV and concealed cameras) is ambiguous or nonexistent.
- Legislated policy on data base surveillance (e.g., monitoring of transactions on computerized record systems and data communication linkages) is unclear.
- There is no immediate technological answer to protection against most electronic surveillance, although there are emerging techniques to protect communication systems from misuse or eavesdropping (e.g., low-cost data encryption).[5]

OTA identified a range of policy options for congressional consideration:

- Congress could do nothing and leave policymaking up to the development of case law and administrative discretion. However, this would lead to continued uncertainty and confusion regarding the privacy accorded phone calls, electronic mail, data communication, and the like, and ignores judicial requests for clarification in areas such as electronic visual surveillance.

---

[3] The data request was sent to all major components within the 13 cabinet-level agencies and to 20 selected independent agencies. Due to the unclassified focus of this study, two Department of Defense components—the National Security Agency and Defense Intelligence Agency—along with the Central Intelligence Agency were excluded from the data request.

[4] Extent of multiple records on the same person is unknown.

[5] Technical options are being addressed in a separate OTA study on "New Communications Technology: Implications for Privacy and Security," expected to be published in winter 1986/87.

- Congress could bring new electronic technologies and services clearly within the purview of Title III of the Omnibus Crime Control and Safe Streets Act, for example by:
  - —treating all telephone calls similarly with respect to the extent of protection against unauthorized interception, whether analog or digital, cellular or cordless, radio or wire;
  - —legislating statutory protections against unauthorized interception of data communication;
  - —legislating a level of protection across all stages of the electronic mail process so that electronic mail is afforded the same degree of protection as is presently provided for conventional first class mail;
  - —subjecting electronic visual surveillance to a standard of protection similar to or even higher than that which currently exists under Title III for bugging and wiretapping.
- Congress also could set up new mechanisms for control and oversight of Federal data base surveillance, for example by:
  - —requiring congressional approval of specific Federal data base surveillance applications (e.g., by statutory amendment or approval of House and Senate authorizing committees);
  - —establishing a data protection board to administer and oversee general statutory standards for creating and using data bases for purposes of surveillance.
- Congress also could amend the Computer Fraud and Abuse Act of 1984 to cover interstate computer crime.
  - —This option, not detailed here, could provide additional legal protection against unauthorized penetration (whether for surveillance or other reasons, e.g., theft or fraud) of computer systems.[6]

Chapters 2 through 5 of this report provide technical and policy analyses relevant to proposed legislation on electronic surveillance and civil liberties, such as the "Electronic Communications Privacy Act of 1985"[7] and the "Video Surveillance Act of 1985."[8]

---

[6] See the computer crime chapter of the forthcoming OTA report on "Federal Government Information Technology: Key Trends and Policy Issues" for discussion.

[7] H.R. 3378 introduced by Rep. Robert Kastenmeier and S. 1667 introduced by Sen. Patrick Leahy. See U.S. Congress, House of Representatives, *Congressional Record*, Extension of Remarks, Sept. 19, 1985, p. E-4128; and U.S. Congress, Senate, *Congressional Record*, Sept. 19, 1985, p. S-11795.

[8] H.R. 3455 introduced by Representative Kastenmeier. See U.S. Congress, House of Representatives, *Congressional Record*, Extension of Remarks, Sept. 30, 1985, p. E-4269.

Mr. KASTENMEIER. Thank you, Mr. Weingarten. I compliment you on your statement and on your work.

I have several questions. They're going to be general questions to get an overview.

You suggested that some years ago a telephone call, or a withdrawal or cashing of a check at a bank, or posting of a letter were distinct and discrete, presumably unrelated activities. However, with the age of telecommunications, they have tended to merge. They all, now, have characteristics in common. Do you think that they can be treated legislatively as a single grouping or do you think that they have to be treated discretely, for purposes of preserving privacy protection?

Mr. WEINGARTEN. It seems based on our study that it is increasingly difficult to distinguish among the variety of communications that take place over a telecommunications network. This problem is compounded by the fact that communications that previously took place on pieces of paper—bank transactions, letters, and so on—are also becoming digitized and transmitted over a network. Technologically, they are indistinguishable, they are all merely data that flow through and sometimes even reside within the network.

There still may be certain kinds of information flows that, because of their sensitivity either to national security or to their tremendous economic value, may require special treatment. I can't think of specific examples in this case, but I would not be prepared to say that all information should be treated the same. There may be some exceptions. At the same time I think, for the bulk of information flow in our society, it is increasingly difficult to make those kinds of distinctions.

Mr. KASTENMEIER. Let me ask you another question about prediction.

We've had, in technology of communications, a move from a more simple system to a very much more complex one; now we're attempting to legislate, at this point in time, confronting this new technology. My question is: With the explosion of change, can we adequately legislate today and have such legislation effective, be contemporary, for very long?

Are there basic principles that we could legislate that would persevere, notwithstanding inevitable changes, in technology in telecommunications?

Mr. WEINGARTEN. I think the approach taken by this legislation, for example, is necessary in order to achieve that goal.

I would hesitate to predict or to state a negative, that we would never have to again address these kinds of problems. It is 17 years since the Omnibus Crime Control Act was passed, and people use the term "already" to describe the need to revisit it. Our ability to predict new technologies gets pretty shaky at the 20-year horizon, so depending on what the Congress means by "long term," it may be difficult to predict that this approach somehow will resolve the problem for that time. In some sense, eternal vigilance seems required. At the same time, this approach seems far more robust, in light of technological change, than past approaches that have tried to define specific paths of information flow.

I should also mention that our study did uncover instances where the courts have had trouble in applying the law to new technologies. That problem is also hard to predict. Sometimes the judicial branch simply does not cope well with trying to take new technological applications and apply legislative language to them in ways that we might think would be——

Mr. **Kastenmeier**. That would seem to suggest an additional burden on us to attempt to clarify policy for the courts.

Mr. **Weingarten**. I would think so, yes, sir.

Mr. **Kastenmeier**. Here is my last question, for the time being at any rate.

You said there's danger that the erosion of privacy was at such a stage that we should really not defer protection. As a matter of fact, I would ask if perhaps in some cases, some technologies, it might not be too late. Might we already encounter difficulties, where you have current accessibility, to try to snuff that out?

For example, let's say people operating scanners are intercepting private cellular conversations, might we be already too late in attempting to reorder what is permissible and impermissible in terms of, let's say, casual interception of electronic communications?

Mr. **Weingarten**. That may be, but I guess I'm not prepared to be quite that pessimistic. In fact, there are two answers one might offer to that question.

In the first place, the need for legislative guidelines and a statement on what is proper or improper behavior may be appropriate even if it is easy to violate. It's easy to steam open an envelop, and it has been relatively easy to tap telephone conversations on copper wire for some time. At the same time, Congress has seen fit to say that should not be done; it is a criminal offense to do that.

Second, the technological controls for securing and protecting communications are advancing. In some ways it is a race: New technologies for communicating come along; new ways to protect those communications also come along. So, I think we should not assume that, a priori, they are, by their very nature, too open to even think about protecting.

Mr. **Kastenmeier**. Thank you, Mr. Weingarten.

I yield now to my friend from Ohio, Mr. Kindness.

Mr. **Kindness**. Thank you, Mr. Chairman.

And thank you, Mr. Weingarten, for your good testimony here.

I would like to explore two aspects of the matter, and ask whether you and your associates have had the opportunity to consider, perhaps in the broader study, either of these matters. One is the international aspect, which might be subdivided into governmental and nongovernmental concerns.

But looking at the nongovernmental side of it for the moment, or principally the nongovernmental side, have you and your associates had an opportunity to explore and determine whether there might be any negative implications associated with restrictions such as we are considering in H.R. 3378? For example, on the sale of information services by U.S. concerns to governments or private concerns in other nations. Realizing that, of course, we already have some problems in that area with other nations that have governmental monopolies on the transmission of information by mail and electronic means.

And the other aspect of that is whether there might be any negative implications for the flow of international trade in information services. I think we're dealing with a somewhat abstract area, because we don't really know what may be developed down the road in those portions of commerce. However, recent years have shown us that we have some problems with other nations in this area of sale of information services, if I may use that term, and, of course, we don't want to create any greater obstacles to advancement in that area.

Is this within the scope of any of the inquiry that you and your associates have made up to now?

Mr. **Weingarten**. It is not covered specifically in this report. At the same time, my program has looked at information policy issues as they interact with other nations in the international regime. In fact, this drawing could have been even more complex because, of course, the U.S. domestic system interconnects internationally. That can create serious problems because each component of the system, then, is under a different regime of law.

It certainly is conceivable, although we don't have any reason to think it is true, that this kind of protection could inhibit trade. I can think of a couple of reasons that we have come across in our work why it might, in fact, help or encourage trade.

In general, foreign countries that have studied and thought about these problems on their own systems tend to be passing very strong rules regarding the privacy of information systems; and, if anything, the United States is being pushed to strengthen those kinds of controls. If those controls are not there may be locked out of certain kinds of markets or certain kinds of service offerings internationally; because our systems are not protected to the degree that, say, the Europeans or Japanese protect their systems.

Second, in my comments I mentioned the danger that if protections are not provided, certain kinds of new technologies might not be developed, because there might not be a market place for them. In-home and office information services—banking, videotex, and so on—might simply not be developed in the United States because consumers, concerned about their privacy, would not use them. If use of cellular telephones were to be inhibited because people were concerned about their privacy, the U.S. development of that technology could also be inhibited; resulting in a negative impact on our trade in these products and services.

Mr. **Kindness**. Let me put it this way, realizing that we're addressing a somewhat indefinite mass of information in itself: I wonder if it is proper, within the scope of your functioning, to ask that as the rest of this more global study proceeds, that your office could make available to this subcommittee any thoughts that may occur to those working in that area with respect to the questions I asked. Perhaps it could be put both positively and negatively, but I think the positive aspects are, perhaps, more apparent.

I was just searching to be sure that we don't find ourselves going unwittingly into an area of negative implication legislatively which is difficult to recognize at this point. With the benefit of the expertise of your office it could be very useful for the subcommittee to consider suggestions that may be even rather indistinct but thoughts that occur to your people who are dealing in this area.

Mr. **Weingarten**. Yes, sir. In fact, the overall study is still going on, and I will go back and talk to my staff about the degree to which we've explored that question in the study. And we would, of course, be pleased to provide written answers to questions that the subcommittee might have based on this testimony.

Mr. **Kindness**. Mr. Chairman, if I may pursue one other area for a moment, I'll try to keep my time down here.

I'm concerned about how realistic we can be in terms of the enforcement of the law as proposed to be changed in a measure such as H.R. 3378. And I'm not being critical of the bill, as a cosponsor I'm quite interested in it. However, at the same time, I recognize that we're very possibly dealing with somewhat unenforceable legal mechanisms, and that the reliance may, indeed, have to be upon protection within the systems that are used, such as scrambling and the like rather than on enforcement by law enforcement personnel or what have you.

In the studies of your office in this area, I would ask whether you have become aware of any developing technologies that could have an effect upon the enforcement side or detection. For example, the obtaining of proof of violation of law and that sort of thing, that may be developing and might be applicable to future law enforcement efforts in this area. Also, whether there are any peculiar problems about detection and providing evidence or proof of violations of the law that have become evident to your office in this study.

Mr. **Weingarten**. We are continuing to look at telecommunications technology and the questions of security and privacy in those systems. We have a new study that has started up in that area, so we will be continuing to look at it.

On the protection side, technology is developing, encryption technology and various other technological controls. I should point out that there are negatives as well as positives from depending on technological protection:

First, if the technology is terribly expensive, it might provide privacy only to those who can afford thousands of dollars for those kinds of protections.

Second, it may deny lawful and legitimate access by law enforcement agencies to the information stream. We have been told that there is some concern that the widespread encryption might deprive law enforcement officials of information necessary to carry out their responsibilities.

Mr. **Kindness**. Thank you very much. And, again, I would suggest that it would be very much appreciated by this subcommittee if, in the pursuit of the remainder of the more global study any further thoughts along this line are developed, we would certainly appreciate the sharing of them. Thank you.

Thank you, Mr. Chairman.

Mr. **Kastenmeier**. The Chair would now like to yield to the gentlewoman from Colorado, Mrs. Schroeder, who is also a cosponsor of the bill.

Mrs. **Schroeder**. Thank you, Mr. Chairman, and I appreciate it.

I don't know if this study went into this, but you mentioned it while you were talking, and that was that other countries have gone further than the United States in protecting these new technologies.

I take it you mean in a legal form; is that correct?

Mr. **Weingarten**. Yes.

Mrs. **Schroeder**. Comparing this bill that we have in front of us, how does it stand up to what other countries have done in that kind of protection of theirs? Is this as strong as, or is it weaker than, or is there any way to put it on some kind of a scale to say whether we're going to then be in parity with other developed nations that are working in this area?

Mr. **Weingarten**. It is very difficult to compare them in that sense of strength, partly because our legislative approach reflects the way telecommunications and information flows in our society and the particular legal regimen that we have regarding it.

I was thinking more in terms of the broader privacy legislation that most European nations have that put fairly stringent controls on access to personal data banks in the private sector. There is no corresponding legislation in the United States.

Mrs. **Schroeder**. So, in other words, their legislation is much more comprehensive than what we're talking about here; is that what you're saying?

Mr. **Weingarten**. It's more comprehensive for certain kinds of information systems. One of the reasons they haven't had to worry about this type of legislation is that the telecommunications systems in most of those countries are monopolies run by the Government, and so one of the problems this bill is addressing is the problem that there is a wide variety of actors in our telecommunications industry.

Mrs. **Schroeder**. Have you looked at how well they've been able to enforce those laws that they do have on the books in other countries? I mean, are they fairly stringent in enforcement?

Mr. **Weingarten**. Our broader study that will be out in a couple of months is doing some comparative work on foreign privacy laws. Some sections of that report will cover data privacy in a broader sense. We will do some comparison. However, it has not been a central focus of our work.

Mrs. **Schroeder**. I realize it's hard to do, but one of the things you keep getting into as you try and approach this is, there constantly seems to be a group of people who think that the law is now passé in trying to deal with this area, that you have to go look to technology instead of the law, that technology, as evidenced by your own charts, has moved way beyond anything that the law can really monitor. And yet, you say other countries have tougher laws than we do on the privacy, and that those laws have been helpful. I think that is important information for us to have as we're talking about updating our laws and making the case that laws are not passé at this point, that technology isn't the only way out of the box.

Mr. **Weingarten**. We are continuing to look at that. It is of increasing importance to the United States in general, whether laws in other countries regarding information—such as copyright and privacy—are inconsistent with U.S. law. Certain kinds of discontinuities and pressures can result, because the telecommunications system is increasingly international and interconnected.

One has essentially a global piece of technology that is covered in different ways in different countries. That starts to affect commerce, the flow of personal information, and relations between those nations. So, it is an important and a growing important issue.

Mrs. Schroeder. Thank you, Mr. Chairman.

Mr. Kastenmeier. Following up on Mrs. Schroeder's question, as I understand your position and the report, it is in support of a bill such as the one before us. As I understand it, it is also to explore policy alternatives which may diverge from the bill, making the bill stronger, if we wish. I think what you have said is, those policy judgments of how far you want to go are really up to us.

You've laid out some options, alternatives to the bill we have before us, with the pros and cons of the changes that might be considered. As I understand that given all things today, you are supportive of the legislation before the committee.

Mr. Weingarten. Well, I have to be very careful, of course, because OTA does not endorse specific legislation, nor do we do legislative analysis, so, we tend to frame our comments very carefully. But our summary is, basically, that if the Congress wishes to maintain those kinds of protections that it has, in the past, decided to provide to the American people, then a comprehensive approach such as the one represented in this bill seems to be about the only technologically feasible way of doing so. It becomes increasingly difficult to draw lines that legislate communication by communication or technology by technology.

Mr. Kastenmeier. Well, on that concluding statement, and noting your inability to support the bill, we certainly accept your analysis, and thank you for your work.

Mr. Weingarten. Thank you very much.

Mr. Kastenmeier. Thank you, Mr. Weingarten, for your testimony this morning.

Next, the Chair would like to call as a witness Mr. Michael Nugent, chairman of the Communications Privacy Committee of ADAPSO. ADAPSO is the computer software and service industry which has 250 member companies. Mr. Nugent is also counsel to the Electronic Data Systems Corp.

Mr. Nugent, during the course of the last many months, has made a number of very helpful suggestions on early drafts of H.R. 3378, and we certainly look forward to hearing his comments today.

I suspect that since the House now has before it a pending quorum call, that rather than interrupt your remarks in midflight, we can defer them for a period of 10 minutes, during which the subcommittee will stand in recess.

Mr. Nugent. Thank you, Mr. Chairman.

Mr. Kastenmeier. The committee stands in recess for 10 minutes.

[Recess.]

Mr. Kastenmeier. The committee will come to order.

At the time the committee recessed, we had greeted our next witness, Mr. Michael Nugent, chairman of the Communications Privacy Committee of ADAPSO.

Mr. Nugent, you may proceed as you wish. We have your statement. You may proceed from it, since it is a relatively short statement, or in any other manner you see fit.

## TESTIMONY OF P. MICHAEL NUGENT, CHAIRMAN, COMMITTEE ON COMPUTER SYSTEMS AND COMMUNICATIONS PRIVACY, ADAPSO, AND GOVERNMENT AFFAIRS COUNSEL FOR ELECTRONIC DATA SYSTEMS CORP., REPRESENTING ADAPSO

Mr. NUGENT. Thank you, Mr. Chairman.

Members of the committee, honorable staff, we thank you for developing this necessary and truly seminal legislation. Electronic Data Systems—I am government affairs counsel for Electronic Data Systems, which is now a subsidiary of the General Motors Corp.—has worked actively in conjunction with ADAPSO, which represents the computer software and services industry. There are about 800 members of ADAPSO. Some 250 of these members are in a section of which I am president, the network-based information services section.

Mr. KASTENMEIER. I might say, for the benefit of the audience and others, that ADAPSO at one time was an acronym for something but currently is not a viable acronym.

Mr. NUGENT. It's kind of like MCI. ADAPSO once stood for the Association of Data Processing Service Organizations. And now, since there are so many different ways of delivering information services, they changed their name. Some of the other associations have great names, but this one is a very strange name; but it reflects the fact that ADAPSO has been around for 25 years, since the service bureau industry really began in the 1956 IBM consent decree.

Mr. KASTENMEIER. They're sort of stuck with the name.

Thank you for that explanation.

Mr. NUGENT. Thank you, Mr. Chairman.

We believe this legislation, even as is—although we are pushing for explicit clarification or expansion—is necessary for the evolution of an information-based economy in society. The lack of the protections accorded by H.R. 3378 and by computer crime legislation—the lack of that computer crime legislation—will retard and will impede the development and the public acceptance of high communicating and processing technology.

The protections in H.R. 3378 should, if broadly applied, prevent customers from losing their privacy rights when they resort, as they must in this day and age, to third-party processors and transmitters of data.

The protections of this bill, if broadly applied, would prevent that loss of business which we have to undergo. In other words, we lose money, we lose the opportunity to make money, when we must shut down, in effect, our computer system to search for records in response to warrants, or subpoenas that are overly broad or just unwarranted.

As a matter of fact, this bill has significant international trade implications. As you mentioned and as Mr. Kindness mentioned, international trade is obviously a high-priority issue.

Some people characterize the privacy rules of other countries as trade barriers. However, we fundamentally believe that these privacy guidelines are attempts to deal with what are problems and historical developments in the various countries.

The Asia-Pacific region has not really developed to a great extent their privacy protection guidelines. Europe has been in the forefront of this. The Organization of Economic Cooperation and Development and the Counsel of Europe each have set down guidelines. Essentially what this means, however, is that if the guidelines applicable in one country are not matched or given equal dignity by the guidelines or rules in another country, then the firm involved cannot process or transmit data outside the country which has the stronger protection rights. So, it is a trade barrier in a sense.

So, for instance, if we wanted to process German data on an Austrian computer, or French data on a United States-based computer, the problem is—one problem that arises—is can that data achieve the same type of protections as would be accorded by French law or German law. So, in effect, this bill is basically saying to our partners overseas that we recognize privacy interests and that we are dealing with them in a very forthright and extensive manner.

Mr. Chairman, those are very general comments about the absolute need for this legislation. This bill grants privacy protections for data in transit, regardless of the technology used, as with EDS, be it microwave, wire line leased from AT&T, satellite services, fiber optics, or et cetera.

This bill grants privacy protections for data in transit, regardless of the nature of the data in transit, be it voice, image, or information, be it personal, corporate, or institutional, and regardless of the regulatory status of the provider of electronic communications service, be it unregulated or common carrier. For instance, EDS has a very extensive international network which is composed, in part, from AT&T's private lines, GTE's unregulated services—although they are a nondominant carrier—as well as our own microwave systems, as well as our own fiber-optics system. This is worldwide, and we're doing this in a very tight time schedule for General Motors and for our own customers.

In granting private protections for data in transit, H.R. 3378 updates the law to reflect how voice, and image, and information are conveyed today, and extends these privacy protections for the electronic communications that we see exist today and for the foreseeable future.

To fully protect the privacy and the sanctity of data of electronic communications, this bill wisely reaches beyond the mere transmission of data, or image, or voice, to information, image or voice data which are stored in connection with the provision of an electronic transmission or communication. H.R. 3378 does this with its unauthorized access and disclosure provisions. In doing so, the bill recognizes that privacy protection for an electronic communication is absolutely meaningless without complementary protection of the electronically communicated data, be it voice, image, or information, while stored along the transmission path or in the computer or communications systems at the originating or terminating point of the transmission.

ADAPSO is here today, Mr. Chairman, and EDS supports ADAPSO in this regard, seeking explicit clarification or expansion of the disclosure and access provisions of H.R. 3378, in order to realistically, and, we believe, fully, apply these provisions and these protections to electronic communications today.

We are looking for expansion or explicit clarification of the phrase "electronic computer systems" to basically include all computer systems used by service vendors to transmit or to process customer data which is electronically transmitted to such system.

We are also seeking explicit clarification or expansion of the bill's access and disclosure provisions to apply to electronically transmitted data, not only while it is in transit to and from the service vendor's computer equipment or in temporary storage along the transmission path, but also while it is stored by the service vendor in connection with the service vendor's provision of a data communication or remote data processing service.

We firmly believe, and it is a problem that is going to be growing as we go through the information age, that our customers should not lose their privacy rights and communication when relying on third party providers of data processing and data transmission services. The results of that, of course, are, we may lose business, so that's why we're here.

Also, our interests in the privacy rights of our customers are tantamount to the privacy interests of our customers, because if we do not accord or deal with these very basic concerns, we may not get the business. Often, the hardware, the software, the technology, is as important to the customer as privacy protection; put it the other way, privacy protection is as important as the service that we perform. So, therefore, we believe that our customers shouldn't lose their rights when they go outside for data processing and data transmission services as they must in this day and age.

In that sense, we would like to have clarified the disclosure and access provisions of H.R. 3378, which are intended to prevent or limit service vendors from divulging electronically communicated information to non-Government parties in response to subpoenaes in civil litigation. If that is not the intention or if that is not the case, we firmly believe that third-party recordkeepers, or third-party recordkeeping provisions, something along the lines of what is included in the IRS Code, should be included. In other words, the customer who is the object of the subpoena should be notified by those seeking the information. That customer should have standing to sue or to otherwise contest the subpoena, and there should be a reasonable opportunity for that customer to deal with this matter.

Those are essentially the summation of our comments, Mr. Chairman. I would be happy to take any comments or questions that the committee may have.

[The statement of Mr. Nugent follows:]

## Prepared Statement of P. Michael Nugent

Mr. Chairman and Distinguished Members of the Subcommittee:

My name is Michael Nugent and I am the Government Affairs Counsel for Electronic Data Systems Corporation (EDS), a subsidiary of the General Motors Corporation. I am here today representing ADAPSO, the trade association for this nation's software and services industry. I am Chairman of ADAPSO's Committee on Computer Systems and Communications Privacy. I am also a Board member of the Association and President of its Network-Based Information Services Section which represents the 250 ADAPSO member companies providing domestic and/or international information management and data distribution services, remote access computing services, remote access database services and electronic mail services.

We welcome this opportunity to address the Subcommittee on this vitally necessary legislation. At the outset, let me express ADAPSO's strong support for H. R. 3378, subject only to the absolute need for clarification or expansion of certain premises and provisions embodied in the bill. Indeed, members of ADAPSO's Privacy Committee have spent many long hours over the past year on earlier staff drafts of this legislation. ADAPSO, of course, has no expertise or experience to relate regarding pen registers or tracking devices.

Before addressing the provisions of the bill, allow me to describe the business activities of this industry which ADAPSO represents.

The member companies of the Network-Based Information Services Section of ADAPSO operate remote access computer systems for the purpose of providing a wide variety of commercial computer-based services to their respective customers. All of these services involve the electronic transmission of data between customer terminals and the vendor's computer system which is operated for the purpose of providing such service.

Some of these services - such as electronic mail services - clearly constitute electronic communication services. Others, however, which also involve the electronic transmission of customer data to and from the computer center, are not so readily classifiable as electronic communication services. This is the case, for instance, where the service consists of the processing of a service order application. In such a case the service customer's sales people use terminals to electronically transmit sales order information from geographically dispersed locations to the service vendor's computer center, at which point the data is made available to the customer's headquarters, factory, shipping, and other facilities for use in the performance of various business functions relating to the order information. These include production and delivery of goods, material ordering, work scheduling, inventory control, shipping, billing, accounts receivable, management, and an almost endless variety of other business management functions.

There are other examples of remote computer services which involve electronic transmission of customer data to and from the venders computer center. These include interactive data services. Such interactive services includes (1) remote access to databases; (2) communicating word processors and work stations; (3) inquiry/response activities between customer terminals and central computer locations, such as status checks for airline flights or financial modeling applications; and (4) transactions such as electronic funds transfers. Data transmission capabilities also are used by the computer service industry to provide bulk data transfer applications. Such applications include transfer of large data files between computers for processing and generation of desired functions (e.g., nightly transfer of billing data from remote locations to a central computer.)

While the services which are performed by means of the transmission and processing of data which are electronically transmitted from and to the customer might not commonly be thought of as electronic communications services, they are functionally indistinguishable. We believe, moreover, that the data which are electronically transmitted to and from the service vendor's computer system in connection with the provision of such commercial services should nevertheless be entitled to communications privacy protection to the same extent as if the service could be more obviously perceived by a lay person as an electronic communication service.

With this background, I now wish to more specifically address a number of provisions of the Electronic Communications Privacy Act.

ADAPSO wholeheartedly endorses and supports the concept of recognizing and protecting privacy interests in electronic data transmissions. Since we believe that the legitimate interest in the privacy of data electronically communicated is the same regardless of whether that data is transmitted for the purpose of receiving a communication service or a data processing service (assuming that it is possible to clearly distinguish between the two), we believe that the term "electronic communication system" as used in Section 102 (a) and (b) of the bill should be broadly defined to include all computer systems which are used by service vendors to transmit or process customer data which is electronically transmitted to such a system. These protections should apply to such data not only while it is in transit to or from the service vendor's computer equipment, but also while it is held by the service vendor in connection with the vendor's provision of a data communication or remote processing service.

It is not clear to us from the current language of the bill, however, exactly what the intent is in this regard. We urge, however, that the ambiguity be clearly resolved in favor of the broad interpretation which includes remote computing service systems within the scope of the term "electronic communication system," and which includes remote computing services within the meaning of the term "electronic communication service."

A contrary construction of this section of the bill would lead to adverse results. If an "electronic communications system" does not embrace all computer systems relying on data transmission, then H. R. 3378 will beg the question of how to distinguish between information or data stored in an "electronic communications system" and information or data stored in a computer system that relies on data transmission to furnish services. We can well imagine that such a result will launch enforcers of H. R. 3378 into the now nearly 20-year old process by which the FCC has tried to draw a bright line between communications and remote data processing. As you know, the Commission has just launched its Third Computer Inquiry.

Another adverse consequence of unrealistic and overly narrow construction of the phrase "electronic communications systems" is frustration of the purpose underlying Section 102. As you have noted yourself, Mr. Chairman,

> "It would be inconsistent to prohibit the interception of . . . information in transit and leave unprotected . . . such information while it is being stored."

ADAPSO has several concerns with the "disclosure" provisions of Section 102. First be assured that this industry which provides information services has no interest in seeking ways to abuse the privacy rights of our customers. That is one of the quickest ways for those of us who have to compete for business, to lose business. The privacy and security of customer information is, more often than not, as important to our customers as the capabilities of the hardware, software and services which are the objects of the transaction itself. Rather, this industry and its customers need legal bases to withstand the ever-increasing quest by government and third parties to obtain access to the enormous amounts and wide range of personal and corporate data residing in our computer/communications systems.

It is not clear, however, whether the provisions of Section 102(b) are intended to prohibit service vendors from divulging the contents of their customers' electronic communications to non-governmental parties in response to subpoenas served in civil litigations, or whether Section 102(b) is intended only to limit the ability of government agencies to require the disclosure of customer data in criminal proceedings. If the former is not intended, then we believe that procedural safeguards similar to the third-party recordkeeper provisions contained in the Internal Revenue Service Code (I.R.C. Section 7609) which give bank customers the right to receive notice of and standing to contest IRS subpoenas which require the disclosure by banks of information about their customers, would be appropriate. Persons who electronically communicate data to a service vendor for the purpose of obtaining communication after transmission or processing services should not be in a worse position with regard to the protection of the privacy of that data than they would be in if they elected instead to use only internal systems to perform the same functions. Otherwise, only those companies who were large enough and financially able to afford to maintain and operate their own private networks would be able to protect their privacy interests, and there would be a definite disincentive to the use of commercial systems, which is definitely not in the national interest.

ADAPSO also suggests that consideration be given to the following specific recommended language clarifications and corrections:

1. at page 2, lines 20 et seq.:

   "(g) It shall not be unlawful under this chapter for any person —

   "(i) to intercept an electronic communication made through an electronic communication system designed for the purpose of making an electronic communication readily accessible to the public.

2. at page 6, lines 1-8:

   The meaning of the words "user" and "authorization" needs to be clarified so as to make clear that the "user" and the party giving "authorization" are, in fact, bona fide customers of an electronic communications service.

3. at page 7, line 7:

   Omit the word "employed" and substitute instead "whose services or facilities are used." This will ensure that providers of service will be permitted to disclose when they assemble a network from different providers of transmission services or facilities.

4. at page 7, line 9:

   The phrase "business activity" should be construed broadly enough so as to include activities related to the maintenance of the security of the electronic communications system. This would permit a provider of service to disclose an electronic communication to law enforcement authorities where the originator of such communication was not a customer of the electronic communications provider, but a hacker or other trespasser.

5. at page 8, line 9:

   The "and" in line 9 should be changed to "or" in order to protect from disclosure not only a record kept by the provider in the course of providing that communication service, but also a record relating to any particular communication made through that service. This will protect not only records generated or created by the service provider, but also records supplied by the customer.

## CONCLUSION

ADAPSO applauds you, Mr. Chairman, Senator Leahy, and your cosponsors for tackling what is a very difficult issue, but one whose resolution is strategically important in the evolution of our information society and economy. You are updating the law to reflect the enormous changes and consequences prompted by technology, technology that has changed fundamentally how much, what and how we communicate. We hope our comments will assist you in consideration of legislation that fully and realistically grants privacy protections to electronic communications. The computer software and computer services industry needs this legislation because our customers need recognition and protection of the privacy interests that ADAPSO has set out before you today. We support your efforts, we welcome H. R. 3378 as truly seminal legislation, and we look forward to continued cooperation and work with your fine staff as this legislation evolves.

In closing, however, I also wish to make it clear that our support of electronic communications privacy legislation is not intended to exclude support of other much needed computer crime legislation. We do believe that in addition to legislation which recognizes and protects fully the privacy of electronic data communications, there is also a need to provide private sector computer systems with criminal law protection against unauthorized computer trespass. In our opinion, however, these are two separate issues, both of which deserve legislative remedy.

Mr. **Kastenmeier**. Thank you very much, Mr. Nugent. We will certainly take under consideration the several suggestions you have made for clarification or for corrections in the language of the bill.

In terms of international trade and the ability for the computer and software industries of this country to compete favorably abroad, do you believe that there ought to be compatibility among the trading nations with respect to privacy laws, just as there is technically among systems employed or, in intellectual property laws, copyright and patents, where the laws of the various nations are either subject to an international convention or at least accommodating with respect to one another?

I take it 3378 wouldn't go that far, would it?

Mr. **Nugent**. No, Mr. Chairman. But I don't think it's necessary, nor have I heard from our folks who are displaying our network worldwide for General Motors and for EDS, saying that incompatibility among privacy rules from country to country is a problem, so long as those rules are explicitly stated. Because there is a very firm recognition that information is power, and there's a very clear concern about U.S. domination of information processing and management within various given countries. It's a very valid concern.

So, the dissimilarity from country to country, in our view, is not a problem. What is a problem, however, is if we want to process data, say, in the United States, for a company or a customer in another country, if our laws are not commensurate in terms of protection with those laws, then we will lose the business. There have been instances where companies have lost business because of privacy dissimilarity in terms of protection.

So, I think the most important part of this legislation and the way it promotes trade is that it gives our trading partners, it gives particularly the Europeans, recognition, and establishment in U.S. law of privacy protection for data.

And that deals not only with unlawful or criminal interception but also Government access. You can imagine how the French Government may feel about United States Government subpoena of our data bases of their budget data. There is a very, very sensitive concern in that regard. So, this law is a very important law in terms of promotion of international matters.

Mr. **Kastenmeier**. One suggestion you made was that, of course, the subject or object of a subpoena involving disclosure of information by a Government agency, private business ought to necessarily involve notice to the target or to the person affected.

Is that a general proposition? Would there be any exceptions if the target were a Mafia member or a suspected terrorist or anything else? Would you make exceptions, or would you say that, no, you ought to adhere generally to the proposition of notice?

Mr. **Nugent**. There probably should be exceptions, Mr. Chairman. And as I've been following different IRS and Treasury attempts to target money laundering and other criminal matters involving, really, bank data; there probably should be exceptions. There are very valid reasons for that. And that's not the problem, because that can be incorporated with the way we do business.

The real problem, and this is particularly for smaller companies, is that there are no rules essentially governing the situation. We need to take their data out of their homes or their buildings in order to truly apply the efficiencies and the cost effective data processing and data transmission. If they lose their rights in that process, then we're going to lose business, and then, also, we will not have any guidelines.

It is sufficient enough of a problem that EDS has built it into their contracts in terms of how we're going to deal with that problem. But it will continue to be a problem as more and more folks realize how much data is being held in third party systems.

Mr. **Kastenmeier**. Thank you for that explanation of your view. I would like to yield to my colleague from California, Mr. Moorhead.

Mr. **Moorhead**. Thank you, Mr. Chairman.

To your knowledge are there any communications technologies that are new, that H.R. 3378 doesn't cover that should be included within the scope of the bill?

Mr. **Nugent**. No, Mr. Moorhead. As far as we can tell, because the terms that are used deal with transmission, which is a function rather than a technology, we believe that all the pertinent technologies have been covered—cellular, wires, private lines leased from regulated proprietors, satellite, fiber optics, microwave. We believe that they are all covered, because this bill has wisely taken the approach of "let's talk about what the function is concerned here, let's not deal with specifics of what kind of technology or what kind of provider is involved."

Mr. **Moorhead**. Do you feel that the remedies that are provided in this legislation are sufficient to ensure the privacy of your customers?

Mr. **Nugent**. We believe so, Mr. Moorhead, but we are trying to get, as you may imagine, broader interpretation of the data which is protected. So, for instance, we get data from our customers for processing. They give it to us electronically, essentially, over any number of facilities. We then send the solutions or the results back to them.

That is not, an "electronic communication" in the sense that we are not selling that, per se, and for its own value; we're using a technology to deliver a service. So, from that point of view, electronic communications and the definitions, et cetera, if thought of in terms of us normal people, the way we look at electronic communications, that may not be included. So, we're trying to see that expanded to include electronic communications of voice, image and information.

Mr. **Moorhead**. Are there ways that you can detect whether people are listening in or tapping in, to access information that should be private?

Mr. **Nugent**. Yes; there are a number of ways. Sometimes it takes some time to detect the problem; but, for instance, many companies in this industry challenge an auditor, an outside auditor, to come in and break their codes and find out what is going on. There are also operational steps, the constant audits at the end of the day.

So, there are a number of steps, both technological and operational, and, I guess, even administrative, which are used to do a check and balance of the systems. Most people get caught, but sometimes it takes a little longer than one would like.

Mr. **Moorhead**. Have any of the members of ADAPSO raised any specific problems with unauthorized accessing of the remote access computer systems that they operate?

Mr. **Nugent**. Probably not. Excuse me, let me step back: I have not heard, in terms of the electronic transmission section of the bill, that that has been a major problem, but primarily because most people assume that it is protected; that is electronic transmission, regardless of the type of technology, regardless of who is providing the service, be it a common carrier or a noncommon carrier.

Because we hold so much information in our computers, that's where we have our problem, both data that sits there and doesn't really go anywhere and data which we are storing and processing for the purposes of transmission. So, the bulk of our complaints have come in the area of the taking of data or the obtaining of unauthorized access, using electronic communications facilities or services to get into our computer systems.

So, we don't have that degree of problem. Most of those complaints would go to the people we do business with, AT&T, GTE, and other providers of services.

Mr. **Moorhead**. Well, they've got some very real complaints, because——

Mr. **Nugent**. Yes; and we share those concerns with them, because——

Mr. **Moorhead**. Advertisements that are being made, promising people that if they buy the services of a particular organization they will be able to eavesdrop.

Mr. **Nugent**. That's right.

And it's getting more sensitive in the sense that technology, the way it is going, you're going to have voice and data on one channel, so to speak, and then you may even have car design data being sent to robots on factory floors. So, the technology is such that all sorts of data and all sorts of purposes are being incorporated within the pipe; no longer is it just for voice or is it just for data, they're all being combined in one facility.

Mr. **Moorhead**. We appreciate you coming and testifying today.

Mr. **Nugent**. Thank you.

Mr. **Kastenmeier**. The gentleman from California, Mr. Berman.

Mr. **Berman**. Are there State laws that now encompass the kind of problem this bill seeks to deal with?

Mr. **Nugent**. Well, I'm not quite sure of the extent of State law. There are some State laws that deal with this, but not as fully as this bill does. And they don't deal with interstate transmission.

And it's really hard to find a network that's not interstate these days; so, there's that problem. There's also——

Mr. **Berman**. Are States preempted from dealing with this problem? Assuming the interception takes place or is organized in the jurisdiction, is there something that preempts the State from doing something here?

Mr. **Nugent**. At this point I don't think so. The FCC, to the extent it has jurisdiction over a question, will preempt any State law which is incompatible and which would impede the development of a network.

Mr. BERMAN. See, I'm thinking of individual State laws, say, on wiretapping or something like that. Are they framed in such terms that they would deal with this kind of interception as well?

Mr. NUGENT. But only within a State. Yes, to the extent there are laws that—and I'm not quite sure of the number of laws that deal with this area. They're not as broad as this law in terms of covering all the types of technology that are being used, and they only deal with the problem on an intrastate level, maybe even a local exchange level.

The real problem, however, is interstate networks, where there are remote computers, for instance; and EDS has about seven or eight major processing centers. And then we transmit data to these centers from all over the country. So, we don't really use an intrastate network, per se, in that sense.

There is also the problem of where is data intercepted. Sometimes it is very difficult to determine that: is it intercepted on this side of the Missouri line or the California line versus that line?

There is also that problem that you could go interception shopping, depending on what the law says from State to State; in other words, get it on the other side.

Mr. BERMAN. I was wondering. I didn't think that a State-by-State solution to this problem would be a viable alternative.

Mr. NUGENT. I'm not quite sure of the extent of State laws that are dealing with this. Computer crime laws, for example; there are a number of computer crime laws on the State level, probably 40 or so computer crime laws.

Mr. BERMAN. I have no further questions, Mr. Chairman.

Mr. KASTENMEIER. The gentleman from Georgia, Mr. Swindall.

Mr. SWINDALL. My only question is, Do you think this will be a difficult bill, once enacted, to enforce?

Mr. NUGENT. I don't believe so, for the following reasons. We have pointed out in our testimony some of the problems with what is electronic communications and what is an electronic communication system.

We think, in some senses, if the law is cut back too far, in other words only deals with data that is in a modem versus in a computer, that you're going to get into what the FCC is getting into, which is now its third computer inquiry. The first one was in the late 1960's. So, that is our—that may pose a problem.

However, when dealing with this in the computer crime context, those who are victimized will bring the case situation to the law enforcement authorities and technology people can explain it. A good prosecutor can make it clear what a computer is to a jury, what a transmission is, what is data when it is stored, when it is transmitted; so we don't think that it is going to be difficult to enforce, particularly if the industry gets behind this enforcement effort.

Mr. SWINDALL. Looking at it from an enforcement perspective, other than the correction that you have recommended in your testimony with respect to the bill, are there any other corrective measures that you think need to be considered at this point with respect to making prosecution of violations more expeditious?

Mr. NUGENT. Well, none come to mind. I know some of the—in the computer crime context again, there have been some concerns with definitions of "access," definitions of "computer." There are some problems with the definition of "user": What is a user? What is a bona fide user? What is authorization?

So, we think we need a legislative history which gives a very commonsense explanation of it; and really, this all can be reduced to common sense, because we're talking about functions and purposes rather than technology or applications of technology.

Mr. SWINDALL. My concern is that when you put criminal sanctions in any bill, you have a much more stringent constitutional test with respect to vagueness. And I'm concerned about potential defenses being raised on the vagueness of various definitions and having the entire case thrown out as a result.

Mr. NUGENT. That's one of our concerns, because we believe even as is, without a broader interpretation or clarification, this bill is an excellent bill which deserves to pass. But one of the problems is, for instance, what is a definition of an "electronic communications system": Is it a communications process or, say, something that does multiplexing, which puts data together for packet switching, or does it also include a computer which receives transmitted data, processes transmitted data, and then sends it on along the path?

So, there are some definitional problems which can be cleared up in legislative history.

Mr. SWINDALL. Well, what I would like to ask you to consider doing is to have some of your folks look at this bill from the perspective that they are now seeking prosecution under it——

Mr. NUGENT. Yes.

Mr. SWINDALL [continuing]. And anticipate now, before we pass this bill, any definitional vaguenesses that we need to address, and supplement your testimony accordingly.

Mr. NUGENT. We will, sir. We've been working with the staff and they're very good to deal with, very open with us. We will.

Mr. SWINDALL. Thank you. I would just rather do it now than later.

Mr. NUGENT. Yes.

And, to tell you the truth, this has been our major problem. This industry has a whole bunch of crazy terms and technologies which may differ from company to company or division to division within a company. So, it's a problem that we continually wrestle with, but there are ways to get clear, readable language.

Mr. SWINDALL. And look at it from a constitutional perspective——

Mr. NUGENT. And from a criminal perspective.

Mr. SWINDALL [continuing]. And from a criminal perspective.

Thank you.

Mr. NUGENT. Thank you.

Mr. KASTENMEIER. I'm sure Mr. Nugent will continue to work with out committee staff to that end, and I appreciate my colleague raising that question.

I would like to now recognize the gentleman from Virginia, Mr. Boucher.

Mr. BOUCHER. Thank you, Mr. Chairman.

First, I would like to commend the Chair for bringing H.R. 3378 before the subcommittee for its consideration.

And, Mr. Nugent, we are very happy to have you with us here today as well.

Mr. NUGENT. Thank you, sir.

Mr. BOUCHER. I know you are aware of the Supreme Court's decision in the *Miller* case, which says that there is no standing on the part of bank customers to block release of their bank records. Our bill, H.R. 3378, takes a very different view and says that with certain exceptions a court order will be required for the release of records. I happen to prefer the approach of the bill, and I would assume that you do as well.

What I would like for you to tell us today is why, from a business standpoint, your company would object to the disclosure of the records of your customers in civil litigation to third parties without notice to the customers?

I think it is helpful for us to know why, from your business standpoint, that is objectionable.

Mr. NUGENT. The disclosure, per se, is not objectionable. The problem is how you disclose and what steps you take without getting your customer mad, and without inviting use of your computer by those who are just looking for information and not paying you for business.

And this particularly applies with the smaller companies. If you get a very overbroad subpoena or a warrant that really isn't based on probable cause, you're literally asking that computer company to shut down that which gives it profit and business to do a search of the records to comply.

I mean, one could take the example of Medicare/Medicaid data, which EDS does extensive processing of. We get a request, for example, to look at all the doctors in the State of Missouri for the last 15 years. We would spend a lot of our computer time, which is what we make money off of, and people, our resources, spending their time. We have no objection, but we would like to have the rules clarified so that we can inform our customer what the rules are. It is a source of irritation in the sense of the uncertainty in this area—who is responsible, who owns the data, whose rights are to be asserted in this case.

I guess a final area is that there is a very real problem in this sense as more and more people, and institutions, and businesses rely on third-party technology. If they get the perception that they have fewer rights, they're going to develop their own systems which will not be as effective, or they will resort to lower level technology, or they will have to lose their rights when they go outside. So, there are some very real problems with what may be considered the real privacy issues.

Mr. BOUCHER. Well, I find your latter point quite persuasive, that under traditional technologies individuals keep their papers and documents in a secure place at their home and their business.

Mr. NUGENT. Yes.

Mr. BOUCHER. And in that context those papers and possessions are protected under the fourth amendment, so the individual can be secure in their possession; but once those items are turned over to a third party and stored in a data bank, present law doesn't extend fourth amendment protections to that storage.

Mr. NUGENT. That's right.

Mr. BOUCHER. And so the absence of that protection creates a disincentive for individuals to use the new technology; would you agree with that?

Mr. NUGENT. Absolutely. Because really, now, the file cabinet is being entered into a computer, so to speak. Now, if it is kept on your premises in a personal computer, perhaps that is a good subject, in terms of data bases, for computer crime. But we believe when it is transmitted electronically to a computer site, then that's part of the process of communication and it should be covered by this.

Mr. BOUCHER. I notice from your testimony that your conclusion is that this legislation before the subcommittee now is compatible with computer crime legislation, both in effect and also being actively considered. I wonder what you would think of this suggestion.

It has been said that perhaps this legislation should be narrowed in such a way that it only addresses the interception of a broadcast signal, while we leave to the computer crime area sanctions against the accessing for improper purposes of a data base. What is your reaction to that?

Mr. NUGENT. Our reaction is basically one of disagreement. The way communications is accomplished these days—

Let me step back. We think that computer crime should deal with data bases that reside within a computer system and go nowhere, and there is a wealth of that occurring either on a PC level or in a mainframe level, where the data that is in the data base doesn't go anywhere. And this would be at the point of the origination or the termination of electronic transmission. But we believe that when data is electronically transmitted for the purpose of processing at another site, then that should be included, because that really is part of the communication process, that is communications privacy. We believe computer crime should deal with this access, unauthorized access, to data bases, we just have a very severe problem with that unrealistic restriction of what is communications.

We really are talking about the sanctity of communications as we communicate today, both in terms of voice and of data. It's very much like a telephone, a telephone just takes the data, which is your voice sine wave, and reconverts that into a digital format and then sends it along to another path. And that, basically, is what is occurring with the computer services business.

Mr. BOUCHER. I gather you think there is some advantage in having in one legislative package, in one section of the code, legislation that pertains both to the receipt of signals for improper purposes and the accessing of data bases for improper purposes, as well.

Mr. NUGENT. It would be a very good sign to the public, and to our foreign partners, and to our customers, and to our industry, that we've got something going.

Mr. BOUCHER. Let me get you to tell us, if you can, about how frequently your records are presently disclosed either to Government investigators or in the course of civil litigation to third parties.

BEST COPY AVAILABLE

And as a second part of that question: What do you presently do to notify your customers that that kind of disclosure is occurring?

Mr. NUGENT. How frequent is very difficult, because we have so much of network data bases involved. It is frequent enough that we have built contract provisions to deal with it. And basically what we do is that as soon as we or even our customers, if our data is on their premises, get a subpoena, they alert us. We then give, at the request of the customer, written request, we will oppose discovery—and, of course, it is at their expense—and will cooperate with whoever is looking for the data.

So, we do deal with that contractually. However, that's always the source of irritation, because the assumption is, "Wait a minute, whose data is this?" And it becomes, sometimes, a very contentious point in dealing with a customer; and not only that, it's very unclear whether this is the way to proceed without Government and especially legislative policy behind it.

Mr. BOUCHER. Let me ask one final question. And I'm asking these questions, by the way, very much as a devil's advocate, because I support the thrust of this legislation and find your testimony with regard to it very helpful.

But why would you say that inscription devices, encoding devices, scrambling devices, would not be just as useful as legislation such as this to address the same goal? Why can't we do technically what this legislation suggests we do through the law?

Mr. NUGENT. Well, we can. Again, part of what we do in terms of selling is not only touting the capabilities of what we're selling, but it's the privacy aspects that are as important to our customer as the functions of what we are doing.

The problem with data security measures is that they are very expensive. Sometimes a transaction, for one reason or another, and usually it is at the customer's request, may not demand that type of expense. For instance, I would wonder how far ATM's would go if they had heavy duty security applied to an ATM transmission from the microcomputer in the ATM machine to the bank's data base.

In other words, we are developing technology that protects the data, but we need a supplement to that technology and a supplement to Federal prosecutorial tools when we deal in this area. We really do need a message from the Government, an unequivocal position, that unauthorized access, interception, invasion of privacy in this new age is still as bad as it was in the old days. And without all that, without that context, it is very difficult to sell to business what you are trying to do.

Mr. BOUCHER. So, to sum that up, you would say that technology can, to a certain extent, help protect the security of a data base, but to make the data base more usable to more people at a lesser cost, we need to pass legislation that will accomplish that result.

Mr. NUGENT. We think so, and we're really kind of caught "between a rock and a hard place" in some areas, and the customer may not insist on the type of privacy protection we think or should be in there. But this would be a suitable overlay, a reasonable overlay, to supplement our efforts and the tools that the prosecutors have to take people to task on these.

Mr. BOUCHER. Thank you, Mr. Nugent.

Thank you, Mr. Chairman.

Mr. KASTENMEIER. The gentleman from North Carolina, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman. I have no questions.

Mr. KASTENMEIER. In which case we thank Mr. Nugent for his testimony this morning. You've been very helpful, as you have been during this entire process working with the committee. Doubtless, we will be in further touch with you as the weeks and months go on.

Mr. NUGENT. Thank you, Mr. Chairman.

Mr. KASTENMEIER. Our final witness this morning is John Stanton, chairman of Telocator Network of America. Mr. Stanton is executive vice president of McCaw Communications Co., which provides mobile communications services in markets in 21 cities across the country.

Mr. Stanton, we are pleased to welcome you here this morning, and you may proceed as you wish. We have your statement, which is, I believe, rather brief. If you like you can proceed from it.

## TESTIMONY OF JOHN W. STANTON, CHAIRMAN, TELOCATOR NETWORK OF AMERICA, AND EXECUTIVE VICE PRESIDENT, McCAW COMMUNICATIONS CO., INC.

Mr. STANTON. Thank you. And good morning, Mr. Chairman and members of the committee.

My name is John W. Stanton. I am executive vice president and chief operating officer of the personal communications group of McCaw Communications. We are a paging and cellular telephony company providing service in a couple of dozen markets, primarily in the West. I am also the chairman of Telocator Network of America. Telocator is our national association for all nontelephone company paging and cellular telephone companies.

I have submitted written testimony to the committee this morning. I'm going to briefly summarize my testimony and then answer any questions that you might have.

In 1968, when the Omnibus Crime Control and Safe Streets Act was passed, my industry was very small. Less than 1 million people were served by pagers. Those pagers were primarily tone only pagers, pagers that just went "beep." Mobile telephony was limited to roughly 100,000 customers that had to, in most cases, use a push-to-talk radio or call-in operator in order to make a telephone call.

Over the last 20 years, technology has revolutionized my industry. Today, we serve over 5 million customers with devices that have been transformed from those that would require a backpack to carry around to those that are very small.

I have brought just a couple of devices, this morning, to demonstrate to you the changes in the technology:

This is a cellular telephone that can be mounted either in a vehicle or carried around, as I've brought it to the hearing room today.

I have also brought a portable cellular telephone that can be conveniently carried around in a pocket. Either of these devices can easily access the telephone network, making calls locally, national, over the interstate or State long-distance network, or international.

The convenience of dialing this phone is just as that of your home or office telephone. The quality of the signals received and sent by that phone are the same as the quality you would except from your home telephone. Many of the customers that we have can't tell the difference between the quality of service that they receive from cellular telephony and the quality that they receive from their home or office phone. And in most cases those people who are receiving calls from someone calling on a cellular telephone aren't aware that that call is being transmitted over radio as opposed to conventional wire line telephone.

In addition, the pagers that were offered for service in 1968, when the Omnibus Act was passed, were roughly the size of the cellular telephone. Most of the pagers in service today are much smaller and conveniently carried around on a belt, such as this digital display pager that is much like the one that I use today. We are just introducing in many of our markets pagers that are so convenient they are the size of a pen that you would carry around in your pocket.

All of these devices have developed and improved in the time since the 1968 act was passed; and yet, due to the judicial interpretation of the 1968 act, while our industry has evolved the law protecting the privacy of my customers has not evolved.

I believe that the privacy of my customers is a basic right. They expect that their rights are protected, particularly as in the case of the cellular telephone call that I described before. I may be calling my office. My secretary may not know that I'm calling from the cellular telephone. She may not realize that her rights to privacy, just as mine, are not fully protected under the current law, because she is not even aware that the call is going over radio waves.

The absence of the law has, and I believe will continue to inhibit the growth of the industry, and inhibit the improvement in technology. Ultimately, for us to be able to offer service to the public at a reasonable cost, it is necessary for us to provide service to a large group of subscribers. The inhibition of the growth of cellular technology and paging technology, forced by the lack of privacy, is unfair because if precludes customers, potential customers, citizens, from getting access to a new technology that will provide service and allow them to live their lives more conveniently and in a better way.

Ultimately, I believe that cellular technology, in particular, represents the bringing together of various kinds of technologies. In his testimony this morning, Dr. Weingarten described in two graphs the increase in complexity of the industry. What I would submit to you is that most of the customers that use those devices that are described aren't even aware of the increasing complexity. They aren't aware that, in many cases, the conversations that 20 years ago were carried exclusively by copper wire are, in many cases, carried by microwave, which the AT&T witnesses, which testified at an earlier hearing, indicated may not be protected by the current law either.

It is the growth of the technology and the need to continue that growth that this bill addresses today. In my opinion, the most desirable role of this law will be to allow the technologies to benefit from the same protection of privacy that conventional wire line telephony experiences, and, therefore, our industry will grow and eventually, in many cases, become a substitute for the use of conventional wire line telephones, but in all cases be able to provide the lowest cost service to the public.

In my written comments, we suggested some slight modifications, most of which can be handled through the report language. Ultimately, in the role of communications technology, 20 years ago the only communications that would be protected by the Omnibus Crime Act are those that are being handled by that beige telephone over on the press desk. Today, these cellular phones and paging devices that are on this desk, here, many of the microcomputers that the reporters here have today, the pagers that the television cameramen have on their belts and many of the members, I'm sure, have, are not protected. And it is the protection of those forms of communication that this bill addresses and that I urge you to take under serious consideration.

Thank you. That concludes my remarks, and I'll be available to answer any questions.

[The statement of Mr. Stanton follows:]

TELOCATOR NETWORK OF AMERICA
COMMUNICATIONS ON THE MOVE

# STATEMENT OF JOHN STANTON
## CHAIRMAN
## TELOCATOR NETWORK OF AMERICA
## BEFORE THE SUBCOMMITTEE
## ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE
## HOUSE JUDICIARY COMMITTEE
## OCTOBER 24, 1985
## HEARING ON H.R. 3378, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Good morning, Mr. Chairman and members of the Committee. My name is John Stanton. I want to thank you for providing me with the opportunity to testify with regard to H.R. 3378, the Electronic Communications Privacy Act of 1985. I am the Executive Vice President of McCaw Communications Companies, Inc., which provides mobile communications services in many parts of the United States.

This morning, I am testifying on behalf of Telocator Network of America. Telocator is the national association of non-telephone company radio common carriers which provide cellular telephone, two-way radio, and paging services to the public.

SUITE 230 2000 M STREET, NW WASHINGTON, DC 20036 (202) 467-4770

According to several recent studies, public demand for paging and cellular radio services is increasing at a rapid pace. Arthur D. Little, Inc., an investment research firm, projects that there will be 10 million pagers in service in the United States by 1990 and that the industry will grow about 2.5 times in the next five years, for a compounded growth rate, in terms of subscribers in place, of more than 20 percent.

Similarly, market studies of the cellular industry predict that there will be 2.5 to 4 million subscribers to cellular radiotelephone service by 1990.

Cellular and modern paging telecommunications services are products of the technology revolution that is still underway. Significant changes have taken place in personal communications services -- changes that were not foreseen in 1968 when the Omnibus Crime Control and Safe Streets Act was passed. That federal act, which would be amended by H.R. 3378, severely limits the circumstances in which an individual's telephone conversation can be intercepted and disclosed. It was passed at a time when telephone conversations were almost exclusively transmitted over wire, from one stationary telephone to another, and pagers were primarily limited to emitting a "beep" tone only[1]. The amount of mobile two-way radio service then was small because the technology was inadequate and few radio channels were allocated for such service. Congress, therefore, designed its statutory protection mainly for the privacy of the traditional telephone conversation.

---

[1] Voice and tone pagers represented 5% or less of paging in the U.S. at that time.

Since then, technology has advanced and hundreds of new channels have been made available for cellular mobile communications to meet the demands of a highly mobile population. Today's sophisticated paging systems are capable of sending alphanumeric messages of 80 or more characters, and similar systems are expected, in the near future, to have the capacity to transmit considerably longer messages. In addition, the Federal Communications Commission (FCC) last year adopted procedures governing the licensing and use of radio frequencies to provide nationwide network paging[2].

Thus, technology has provided us with entirely new modes of communications. Yet, recent State Supreme Court decisions have held that communications received over radio are not "wire communications" within the meaning of Title III of the Omnibus Crime Control and Safe Streets Act[3], thereby denying privacy protection to one of the fastest growing segments of the communications industry. These judicial decisions are based on the technology involved -- radio technology was not accorded a reasonable expectation of privacy because the technology made it easy to eavesdrop. However, the general public does not distinguish between a telephone conversation transmitted by wire or by radio in terms of privacy. The right of privacy is a fundamental right irrespective of the means by which the message is carried.

[2] A network paging system would enable a subscriber to receive pages when traveling outside the local service area.

[3] *Rhode Island v. Delaurier*, 488 A.2d 688 (R.I. 1985)

It is, therefore, incumbent upon Congress not to alter certain privacy expectations, but to develop legislative guidelines so that national policy may keep pace with technological advancement. Failure to modernize the privacy statute to account for new technologies and services could discourage use of mobile communications services, thereby stifling emerging industries and limiting the benefits of enhanced mobility of telecommunications to the public.

The Federal Communications Commission (FCC) also expressed its concern about the privacy issue last year in the Nationwide Paging Service proceeding as follows:

> ...we would like to express our concern about the privacy of subscribers using alphanumeric paging equipment....these systems are vulnerable to interception by undesired third parties and the messages conveyed are easy to store and sort with computers. This can pose a threat to the privacy of subscribers. While we do not have a record at this point on which to propose a specific action, we would like to point out to the operators of all sophisticated paging systems our concern in this area...

For these reasons, Telocator Network of America supports the need for legislation such as H.R. 3378. The Electronic Communications Privacy Act would provide the crucial legal protection necessary to prevent unauthorized access or interception of electronic communications, including cellular telephony and paging. It would bring the United States Criminal Code up to date with the electronic revolution and establish criteria so that privacy protection can catch up with technology.

While Telocator heartily supports the broadening of Title III privacy protection to include electronic communications, several provisions in the legislation, as introduced, may be cause for concern. For example, H. R. 3378 would exempt from privacy protection communication systems that are "readily accessible to the public". Because over-the-air radio transmissions can be intercepted, this somewhat vague exception from protection could be construed to cover, for example, cellular communications which the legislation is otherwise intended to protect.

Also, the bill prohibits the installation or use of "tracking devices" without a court order. Presumably, this prohibition is intended to reach only those devices that are used solely or primarily to track persons or objects. However, the definition of the term "tracking device" in the current bill is broad enough that it could be read as including paging or cellular equipment.

Telocator believes that these provisions can be easily clarified without impairing the basic purpose of the legislation and we are ready to work with the Subcommittee and staff in crafting any necessary modifications to the bill.

In summary, Telocator Network of America strongly endorses the expansion of privacy protection to electronic communications as embodied in H.R. 3378 and we would like to thank the Chairman for his continued efforts toward this end.

Thank you for allowing me the opportunity to testify this morning. I will be happy to answer questions at this time.

Mr. **KASTENMEIER**. Thank you for that most interesting presentation, brief as it was.

What is the basic difference between the walkie-talkie of World War II and the technology used in the contemporary cellular telephone, the portable telephone that you've referred to?

Mr. **STANTON**. The walkie-talkie of World War II utilized one radio channel and was obviously extraordinarily large. A number of technological developments over the last 40 years have come together to produce this telephone.

The two most important technological developments are the development of the microcomputer technology, which will allow in a highly miniaturized form this radio to automatically select any one of 666 radio channels over which the conversation will take place. That microcomputer, combined with the second technology, that is the miniaturization of both transceiver and battery technology, has allowed us to introduce a cellular phone, this phone is roughly 28 ounces, and phones that we will be introducing before the end of the year are roughly 15 ounces, so that miniaturization and, in particular, the reduction in the weight of the units, have been the most important changes that have occurred in the last 40 years.

The one other change I might point to is not a technological change as much as a regulatory change. The radio spectrum available for the use in the radio common carrier industry was very limited, really, until just the past few years. The FCC has recently made available a number of paging channels and cellular channels over which two-way and one-way communications can be offered, and it is the growth of the number of channels that has increased the number of competitors, and, therefore, also the innovation in the business.

Mr. **KASTENMEIER**. You heard the preceding witness, representing ADAPSO, talk about European efforts to protect the privacy of some telecommunications. Can you tell us whether that would have included cellular telephones, paging devices, and the technology that you represent?

Mr. **STANTON**. I can't speak with authority as to the particulars of the European laws. I can tell you, however, that most of the European countries either have implemented or are in the process of implementing the cellular systems of some configurations utilizing either the American technology or slightly different technologies.

It is my understanding, in particular from the comments of the representative from ADAPSO, that their communications privacy laws would protect them, although it would have to be something that our staff would have to get back to you and your staff on in more detail.

Mr. **KASTENMEIER**. Yes; I would appreciate once you've determined the answer to that question, if you would get back to us.

Mr. **STANTON**. We would be happy to.

[The following information was subsequently provided to the committee:]

Currently, many European countries have more stringent statutes with regard to record systems protection than the United States does. However, communications privacy does not enjoy the same protection. For example, in England, where cellular systems are just going on-line, a spokesperson for one of the two licensed cellular systems reports that privacy protection is one of two top objectives for cellular system providers (the other being spectrum allocation).

Mr. **Kastenmeier**. The OTA report assessing the impact of emerging technologies on privacy obviously did include cellular telephones.

In light of the relative ease with which such calls can be intercepted by scanners and regular radio, is it realistic in your view to provide statutory protection?

Mr. **Stanton**. From our perspective the key issue really is one of establishing national policy. The privacy of wire communications has always been respected and understood; the protection afforded to a user of cellular technology has not always been understood and is not, today, understood.

I was just on the plane on the way in last night, reading an article from the Boston Globe that described in almost frivolous detail a conversation between a boss and his secretary, and in that conversation, itself, the customers would have expected to be protected, but it's apparent that they were not protected, for the privacy of the conversation.

You cannot, I don't believe, legislate any perfect world or produce for us an environment in which the privacy of our customers is absolutely protected; but by establishing a national policy that clearly identifies the intent of the Congress to protect cellular communications and other forms of communications from illegal access, a statement can be made and penalties can be established that then can be worked with.

Mr. **Kastenmeier**. Early last year the Office of Legal Counsel of the Department of Justice concluded that there were at least three kinds of pagers, and that the nature of the legal protection afforded each of them depended on the technology involved. For example, one, the tone-only pager, required no court order to be intercepted; two, a tone and digital read-out pager, required a search warrant based on probable cause; and three, a tone-and-voice pager, required a title 3 court order before it could be intercepted.

Does this differentiation, in your view, make good sense? Or should we have legislation to change this outcome?

Mr. **Stanton**. In my view all of the types of pagers really should be protected. But from a simply practical point of view, the analysis of the Department of Justice seemed to miss one salient point, and that is, in virtually every market in the country, including this one, a single frequency is used to provide service to all of those kinds of pagers. So, this pager, which uses the 158.7 megahertz frequency, commonly known as P6, provides services to this digital display pager; it also provides service to tone-and-voice pagers; it also provides service to tone-only pagers, as well as a new kind of pager that is only peripherally addressed, in that analysis, in an alpha-numeric display pager, in which a customer receives an alpha-numeric printout of numbers and characters.

All four of those kinds of pagers really are carried over the same frequency; and as a result, if you intercept a tone-only pager, you're also going to intercept tone-and-voice pagers, you're also going to intercept digital display and alpha-numeric display pagers. So, to provide protection only to tone-and-voice pagers is really to provide protection to all of the types of pagers; but, conversely, to give access to a paging frequency that allows tone-only pagers in effect violates that standard of giving people access to a tone-and-voice pager.

Mr. KASTENMEIER. Your conclusion is that we need to protect each of the technologies involved in a similar fashion; that is, they're all part of the same family which require protection.

Mr. STANTON. In effect—it would be like saying that for some reason you could not read the sports section of the newspaper but you could read the classified ad section of a newspaper. If you buy a newspaper, you get the whole paper, and it's kind of tough to differentiate once it's in someone's possession, what pages that person would read.

Mr. KASTENMEIER. Thank you.

I would like to now yield to the gentleman from North Carolina, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman. No questions.

Mr. KASTENMEIER. The gentleman from Virginia, Mr. Boucher.

Mr. BOUCHER. Thank you, Mr. Chairman.

I was very interested in the chairman's first question, and I would like to follow up just a bit on that with you.

A lot of individuals who own scanners and I understand there are millions of them nationwide have focused on this suggestion that we prohibit the interception of cellular telephone call signals, which, of course, can be picked up just on regular scanners.

Now, if we do that, aren't we going to be criminalizing the conduct of millions of people, who, if they just happen to turn the dial one notch too far and pick up a cellular telephone call, are then committing a crime? Isn't that a problem?

Mr. STANTON. Initially, it seems to me that the issue is one of national policy. That is, should the conversation that people expect to be private be protected by the privacy legislation? And my answer, as I've made clear today, is unequivocally yes.

There are technical issues that we don't need to go into in detail here, that many of those scanners to which you refer really cannot access, or do not access, the cellular frequencies today. And, in particular, it is very difficult, and it requires a new kind of scanner that has only been introduced in the last few months to really effectively access the cellular frequencies. Because, in effect, this phone uses two frequencies at the same time, one for the conversation to go from this phone to the base station and one for the conversation to go from the base station to the phone, and you really have to intercept both. But it's only scanners that do that that really are effectively handled, and there are very few of those scanners that are out so far.

Mr. BOUCHER. Let me just stop you at that point.

When you say "very few out so far," the information that I had, and perhaps it's incorrect, is that there are millions of scanners in common usage today that have the capacity to intercept cellular telephone calls; is that not correct?

Mr. STANTON. They have the capacity—many of them, not all of them, had the capacity to intercept one-half of a cellular call, but not necessarily receive both of them. Nonetheless, half of the protection of privacy, it seems to me, is as important as complete protection of privacy.

Mr. **Boucher**. But I understand your suggestion to be that any interception of a cellular telephone call, whether it be from one party or the other, would be criminalized; is that not correct?

Mr. **Stanton**. I guess, frankly, the fact that those people use scanners to eavesdrop does not in any way legitimize that behavior; so, I guess the simple answer to your question is "Yes, it would."

Mr. **Boucher**. Well, I understand your concern, and, frankly, I share it; but I also sense some very serious technical problems with the enforcement of such a broad provision. And it occurs to me that perhaps we should examine two other alternatives.

The first of those is some sort of encryption by the cellular system, itself, of the signal. And I notice that new technology now makes that available. AT&T has a pamphlet here indicating that encryption can be provided.

I would like to get your comments on why it isn't simpler, given the fact that millions of people own scanners that could, inadvertently even, intercept a signal which would then be declared criminal under this legislation, why can't we use this instead; isn't this a simpler approach?

Mr. **Stanton**. The legislation clearly is not a substitute for encryption; nor is encryption a substitute for legislation in my opinion.

McCaw Communications has contracted with AT&T to be one of the first office applications for the encryption devices described in the pamphlet you held up. It will be introduced in one of our markets later this year.

There are some technical problems with it, primarily that the conversations can be somewhat scratchy using the encryption devices, and those units that have the encryption device have a difficult time conveniently roaming from system to system; which is one of the chief attributes of the innovation of cellular, that is a national system. And encryption does inhibit them.

But many of our customers, particularly State governments, the Department of Defense, large contractors such as Boeing, are very concerned about the privacy of the conversation and are willing to work with us on the encryption devices. We are, therefore, going to offer it to customers that make that request; but frankly, it is at a substantial cost.

The investment per customer, for those customers demanding encryption, will be roughly 30 percent more for the base station and switching unit and 100 percent more for the phone itself. As a result the customer is going to have to pay much higher rates in order to enjoy the benefits of that privacy.

And I guess I would just pose a policy question as to whether privacy should be available only to those people who can afford it and those people who can use it. It seems to me that the desirable thing to do is to have the two go hand in hand.

We will, and we are introducing encryption for those people who can specifically use it and are specifically willing to accept the disadvantages of the somewhat scratchy transmission and the problems of both cost and limited roaming. But it seems to me that all of our customers, regardless of whether they can afford encryption devices or not, should be afforded the privacy that this legislation provides.

Mr. BOUCHER. Well, I'm pleased to hear that encryption is, perhaps, a partial answer to the problem, and I'm glad to hear that the technology is coming forward to do that.

My concern that we may criminalize the inadvertent behavior of a very large number of people who accidently happen upon a channel where there is some broadcast of a cellular call still concerns me. And another possible way to address that is to refine the definition of what is criminal in the statute.

Now, I know that the State of California, in adopting a State law on the subject, has indicated that the only conduct which is criminal is the interception of the signal for, I believe they say, malicious purposes. What would you think about having that kind of definition in the Federal legislation?

Mr. STANTON. I have seen the California law. I would be reluctant to give you a definitive opinion on whether it addresses all of the concerns.

I guess from my perspective the key is to inhibit behavior that is simply undesirable from a policy point of view. The notion that that information can't be used against someone or in some way, as described by the California law, takes us part way, clearly is not, however, adequate, in my opinion, given that you can inadvertently obtain information. Imagine a stockbroker, for example, or a businessman calling his stockbroker and saying, "buy this stock, I have this information, this is going to be happening," and, thus, that kind of a conversation could be inadvertently intercepted and used against someone.

We provide service in Austin, TX. There's been a great deal of controversy, recently, because the existing two-way service that is being provided and being used by some State legislators in Austin has been intercepted by local folks in order to get a jump on what legislation is going to be happening, is going to be proposed and introduced, and also, apparently certain private conversations that were somewhat embarrassing were made available in the public press. The point is that everyone should have the right to privacy whether or not that information is used.

Mr. BOUCHER. Well, I think your answer is a good one. I'm not sure that I'm entirely satisfied by it.

I think we have two values that conflict here. On the one hand we want to stimulate to the greatest extent that we can the use of cellular calling, because that is a technology that I think millions of people can enjoy. On the other hand, we want to make sure that the inadvertent conduct of people who own scanners, in simply happening across a channel that contains a cellular call in transmission, is not made criminal. And I think that is something we'll carefully have to weigh, and your advice today is most useful. Thank you, sir.

Mr. STANTON. Thank you.

Mr. BOUCHER. Thank you, Mr. Chairman.

Mr. KASTENMEIER. On the point of a typical CB broadcast or communication from a car, can it not act as a scanner for purposes of intercepting cellular telephone calls?

Mr. STANTON. It does not.

Mr. KASTENMEIER. It does not.

Mr. STANTON. And most of the scanners that are available today primarily access those CB frequencies. The cellular frequencies are in the 800-megahertz spectrum band. As I indicated, two radio channels are used for every conversation, and as a result the number of scanners that are actually used for or could conceivably access the cellular frequencies is fairly limited.

I'll make sure that our people get back to the staff with more information as to the scope of that.

[The following information was subsequently provided to the committee:]

Three companies comprise approximately 95 percent of the scanner manufacturing industry. Of those three, only one company has a scanner on the market capable of scanning the 800 Mhz band for cellular frequencies. That particular model has been on the market for less than 6 months and sales figures are currently unavailable.

Mr. KASTENMEIER. Scanners may also be used news rooms for news gathering purposes. This may raise another question: Is there some first amendment right in using scanners to find breaking news?

Have you considered that question, the relationship of scanners in used in the news gathering process versus the privacy of persons with the cellular devices and others who would have an expectation of privacy?

Mr. STANTON. I am not an attorney, and I'm not in a position to give you an opinion on first amendment rights. I guess I could only comment in terms of a couple of our customers.

We have newspapers that are customers to our services in Seattle, Portland, Oklahoma City, Kansas City, and those newspapers, I think, expect a certain amount of privacy in utilizing their phones to transmit data, transmit stories back to their newsroom, that they expect will not be intercepted.

And, in a sense, it would seem to me that while your question poses a first amendment question that would suggest open access to the radio waves, it would seem to me that there are some first amendment issues that would suggest that, in fact, the radio waves should be protected in privacy to protect those stories before they are printed so that the newspapers enjoy the freedoms that they've always enjoyed.

Mr. KASTENMEIER. Thank you very much, Mr. Stanton, for your testimony today. You have been very helpful, and obviously there is high interest in the technology that your industry represents; the expectations for it are almost limitless. To the extent that privacy is involved and new laws can be considered which positively affect that area of communications, you are playing an obviously important role. This committee would expect to be in further touch with you.

Mr. STANTON. Thank you, Mr. Chairman and members.

Mr. KASTENMEIER. This concludes this morning's hearings on telecommunications privacy and on the bill H.R. 3378. There will be a further hearing, possibly two hearings, in the near future. Until that time the committee stands adjourned.

[Whereupon, at 12:25 p.m. the subcommittee was adjourned.]

BLANK PAGE

# ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

THURSDAY, JANUARY 30, 1986

House of Representatives,
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice,
Committee on the Judiciary,
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:10 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier, Berman, Boucher, Moorhead, Swindall, and Coble.

Staff present: Deborah Leavy and David Beier, assistant counsel; Joseph V. Wolfe, associate counsel, and Audrey K. Marcus, clerk.

Mr. Kastenmeier. The committee will come to order.

This morning the subcommittee is conducting the third day of hearings on the Electronic Communications Privacy Act of 1986.

During today's hearing we will be hearing from representatives of telephone companies, radio users and hobbyists and a manufacturer of radio scanner equipment. It is my hope that through these hearings the committee will obtain greater insights into the strengths and the weaknesses of this legislation.

As the testimony of the witnesses will demonstrate, the subject matters that are covered in the legislation are as diverse as they are complex. During the course of our deliberations we have learned a great deal about the array of new communication technologies. The very complexity of these communications techniques may mean that inevitably there will be conflict among stakeholders in the communications process.

For example, it is clear that the users of cellular telephones desire that their communications be protected against interception. On the other hand, hobbyists and others who use and operate radio systems want to be able to freely use the radio spectrum. These radio operators claim that the use of scanners and other devices inevitably result in interceptions, for example, of cellular phone calls.

These two groups of people have differing and conflicting interests. It is our task to reconcile these conflicts. One way of accomplishing this task would be to make inadvertent interceptions lawful. Another approach would be to require a minimum level of encryption before cellular telephone calls are afforded statutory protection against interception.

So, these conflicting interests are important and deserve our attention. I wish to assure those with an interest in this bill that before this bill reaches the end of the legislative road the views of all affected constituencies will be heard. It is possible—perhaps likely—that some interested parties will differ with the policy judgments that this committee makes. These differences of opinion will nonetheless inform our deliberations.

This morning I would like to begin with a panel of two witnesses. First, Mr. Neal J. Amick of American Telephone & Telegraph. Mr. Amick is a specialist in corporate security for AT&T. He also has a background in law enforcment.

Also on our first panel is John Kelly, an attorney with Southwestern Bell, a regional Bell operating company. Although Mr. Kelly does not represent all seven regional Bell operating companies, let me say that all seven have submitted their comments to the committee and, without objection, they will be made part of the record.

Also, without objection, consent will be granted that the meeting today may be covered in whole or in part by television, radio broadcast, and/or still photography, pursuant to rule V of the committee rules.

Gentlemen, Mr. Amick and Mr. Kelly, if you would come forward. Mr. Amick, we will call on you first. I know that you have extensive statements together with appendices. Without objection, your statement in its entirety together with the appendixes, will be received and made part of the record, and you may proceed as you wish from your own statement or you may summarize your views if you wish.

## TESTIMONY OF NEAL J. AMICK, DIVISION MANAGER FOR CORPORATE SECURITY, AMERICAN TELEPHONE & TELEGRAPH CO., AND JOHN W. KELLY, JR., ATTORNEY, SOUTHWESTERN BELL TELEPHONE CO.

Mr. AMICK. Thank you, Mr. Chairman, distinguished members of the committee.

My name is Neal Amick, division manager—corporate security for the American Telephone & Telegraph Co.

My organization's responsibilities include the protection of the privacy of AT&T's own communications and those of its customers. In this capacity we interface with local, State, and Federal law enforcement officials seeking access to AT&T's records and facilities, and we regularly deal with the provisions of title III of the Omnibus Crime Control and Safe Streets Act of 1968, which would be amended by H.R. 3378.

It is an engrained principle of AT&T's corporate culture that our customers are entitled to use our facilities with the same degree of privacy that they would enjoy in face-to-face discussions, and that any deviation from this principle would seriously impair the usefulness and integrity of our services.

Mr. Chairman, in summarizing H.R. 3378 at its introduction, identified seven major features. My remarks will address each of them in turn.

The first major feature is an extension of the protection against interception from voice transmission to virtually all electronic communications. AT&T wholeheartedly supports this objective. We have, however, suggested to your staff some minor clarification and a broadening of the bill's definition of the word "intercept."

The second major feature of the bill is an extension of protection to private as well as common carriers. As a common carrier, a user of remote computer services, and a transmitter of our own proprietary data over internal corporate networks, AT&T supports this change as well.

The third major feature is the creation of both criminal and civil penalties for persons who, without authorization, obtain or alter a communication stored in an electronic communications system. AT&T believes that the language employed requires some expansion as the operations of a hacker or saboteur that may not amount to the obtaining or altering of a stored electronic communication can result in a costly interruption or denial of access to customers and service providers.

For example, by altering the service provider's software, access to the system can be partially or totally blocked.

We further believe that the provision would be much more effective if it were clear that access can be authorized only by users who are themselves authorized, and that the obtaining or altering even a portion of a stored communication would be unlawful.

The fourth major feature of the bill provides that an electronic communication service may not disclose to a governmental authority its records concerning a communication unless the governmental authority obtains a court order for such disclosure.

AT&T believes there must be exceptions to this prohibition for each of the following three situations:

First, with the consent of one party to a communication made in the furtherance of a criminal act, such as extortion, kidnaping, or a bomb threat.

Second, communications consisting of an abuse of service or other illegal act, including obscene calls, theft of communication service, and computer abuse.

Third, communications indicating a threat to life or property—when a missing child calls for assistance or an elderly person collapses while talking on the telephone to an operator.

The fifth of the bill's major features expands a list of crimes for which an interception order may be obtained.

AT&T supports these changes and suggests also including violations of 18 United States Code section 1030 on computer crimes, and section 2511 on interception of electronic and oral communications be added to the list of those crimes.

The sixth major feature involves updating the wiretap laws basic provisions and includes the addition of a provision that no order may require the participation of any electronic communication system employee in the physical entry into a suspect's premises in order to install a bug or tap.

AT&T wholeheartedly supports this portion of the bill.

As its seventh and last major feature, the bill would add new provisions prohibiting the use of pen registers and tracking devices without a court order.

We recommend that there be an exception permitting service providers to use pen registers in protecting themselves against fraud or abuse of their services or customers.

The new provisions also contain a requirement that common carriers afford technical assistance to accomplish the installation of pen registers or tracking devices when a law enforcement officer determines that an emergency exists. In this case, a carrier is required to act at its peril since there is no way to determine whether the officer's assessment is justified.

We urge that a provision be added to the bill making a good faith reliance on such an assessment a complete defense to any civil or criminal action brought against the carrier or any of its employees.

My comments today have necessarily been broad brush in nature. We have recommended other important changes to the bill and they are described in the appendix to my written statement.

We appreciate the opportunity to participate in these early stages of the legislation. Mr. Chairman, that concludes my prepared statement. I would be happy to answer any questions as appropriate.

[The statement of Mr. Amick follows:]

## PREPARED STATEMENT OF NEAL J. AMICK

Mr. Chairman and Distinguished Members of the Subcommittee:

My name is Neal Amick. I am Division Manager for Corporate Security at American Telephone and Telegraph Company, a leader in the provision of voice and data transmission products and services.

My Organization's responsibilities include the protection of the privacy of AT&T's own communications and those of its customers. In this capacity we interface with local, state and federal law enforcement officials seeking access to AT&T's records and facilities, and we regularly deal with the provisions of the wiretap law passed by Congress in 1968,* which would be amended by H.R. 3378.

Our communications protection efforts within AT&T have for many years involved a vigorous employee compliance program centered around a code of conduct that is republished and redistributed annually to all of our employees, of which there are currently over 350,000. As a result, it has become an ingrained principle of AT&T's corporate culture that customers are entitled to use our facilities with the same privacy that they enjoy in face to face discussions, and that any deviation from this principle would seriously impair the usefulness of our services.

---

* Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

For protection against external interception of communications, AT&T substantially relies on the deterrent effect of the existing wiretap law. We reinforce this deterrence by actively supporting the prosecution of violators.

But as the Chairman observed in introducing H.R. 3378, "new modes of communication have outstripped the legal protection provided under statutory definitions bound by old technologies." The protection against the unauthorized "aural acquisition" of the contents of a communication that was enacted in 1968 appears anachronistic when it is applied to AT&T's business today.

AT&T is not only a provider of public switched, private line and data services, but it is also engaged in the management and processing of information and the provision of computer-based systems. In supporting its network, AT&T maintains over 40 million lines of computer software. Our 4ESS switching systems, today's largest, processes over 700,000 communication calls per hour by means of an AT&T central computer that has over a million lines of software instructions. Our computer systems (e.g., the 3B line of minicomputers), information networks (e.g., Common Channel Interoffice Signalling and Information Systems Networks), management information systems (e.g., System 75 & 85) and switching systems (e.g., No. 5ESS) provide a variety of products, networks and services to handle our customers' information needs.

From the vantage point of our telecommunications operations we have observed that the dissemination of data, electronic mail, graphics, and other non-voice communications is ever-increasing and rapidly becoming indistinguishable during transmission from voice communications. As an example, most long distance systems, and a growing percentage of local systems, digitize voice signals for improved transmission speeds, storage and processing.

AT&T therefore enthusiastically supports H.R. 3378's expansion of wiretap law protection to digital, data and other non-voice communications. At the same time, however, we believe that the bill requires a number of revisions if it is to be fully effective in protecting electronic communications and fully workable from the standpoint of electronic communication service providers.

The Chairman, in summarizing the bill at its introduction, identified seven major features. My remarks today will address each one of them in turn.

The first major feature of H.R. 3378 is the extension of the protection against interception from voice transmission to virtually all electronic communications. AT&T wholeheartedly supports this objective but believes that a better definition is required for the word "intercept," which is the obvious linchpin of the provisions making it unlawful to intercept electronic or oral communications. The H.R. 3378 definition is ambiguous because is involves the definition of a term with a derivation of the same term. It reads:

> "intercept" means the interception of the contents of any electronic or oral communication through the use of any electronic, mechanical or other device."

We recommend that the word "interception" be replaced with a series of words that would include, as a minimum: acquisition, reception, recording and copying. We also recommend that the word "contents" be deleted because the person who intercepts a digital message and leaves its decoding for another would not be intercepting the "contents" of the message under the 18 U.S.C. § 2510(8) definition of the term. Finally, we recommend that the definition of "intercept" be reworded to include the interception of any portion of a communication.

The second major feature of the bill is the extension of protection to private carriers. At present only common carriers are covered by the wiretap law's protection of wire communications. As a business corporation that is a common carrier, a user of remote computer services, and a transmitter of its own proprietary data over internal corporate networks, AT&T supports this change wholeheartedly.

The third major feature is the creation of both criminal and civil penalties for persons who, without authorization, obtain or alter a communication stored in an electronic communication system. As the Chairman has pointed out, it would be inconsistent to prohibit the interception of digitized information while it is in transit and leave unprotected the accessing of such information while it is being stored. The provision in question reads as follows:

> (3) Unless authorized by the person or entity providing an electronic communication service or by a user of that service, and except as otherwise authorized in section 2516 of this title, whoever willfully accesses an electronic communication system through which such service is provided or willfully exceeds an authorization to access that electronic communication service and obtains or alters that electronic communication while it is stored in such system shall --

(A) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain --

(i) be fined not more than $250,000 or imprisoned not more than one year, or both, in the case of a first offense under this subparagraph; and

(ii) be fined not more than $250,000 or imprisoned not more than two years, or both, for any subsequent offense under this subparagraph; and

(B) be fined not more than $5,000 or imprisoned not more than six months, or both, in any other case.

AT&T believes that the language employed by the bill requires some expansion and clarification. The language does not take into account the fact that the operations of a hacker or saboteur that may not amount to obtaining or altering a stored electronic communication can result in a costly interruption or denial of access to customers and service providers. (For example, by altering the service provider's software, access to his system can be partially or totally blocked.) We further believe that the provision would be much more effective if it were clear that access can be authorized only by users who are themselves authorized, and that the obtaining, etc. of even a portion of a stored communication would be unlawful.

We therefore recommend that the provision be revised so as to apply to one who, not having received authorization from the service provider or from an authorized user, "obtains, alters, or interrupts or prevents access to, an electronic communication, in whole or in part, while such communication is stored in the system." We also believe that internal numbering should be employed for improved clarity. Our proposed version is as follows:

> (3) Unless authorized by the person or entity providing an electronic communication service or by a user of that service acting within the scope of authority granted by such person or entity, and except as otherwise authorized in section 2516 of this title, whoever (i) willfully accesses an electronic communication system through which such service is provided or willfully exceeds an authorization to access that electronic communication service and (ii) obtains, alters, or interrupts or prevents access to, an electronic communication, in whole or in part, while the communication is stored in the system shall --

The fourth major feature of the bill provides that a provider of electronic communication service may not disclose to a governmental authority its records concerning a communication made through its service unless the governmental authority obtains a court order for such disclosure. AT&T believes there should be exceptions to this prohibition that would permit disclosure without a court order for each of the following situations:

a) With consent of one party to a communication made in furtherance of a criminal act (e.g., extortion, kidnapping, or bomb threat).

b) Communications constituting an abuse of service or other illegal act (e.g., obscene calls, theft of communication service, computer abuse).

c) Communications indicating a threat to life or property (e.g., a missing child calls for assistance or an elderly person collapses while talking to an operator.)

The fifth of the bill's major features is its permitting Acting Assistant Attorney Generals (as well as Assistant Attorney Generals) to approve interception applications and its expanding the list of crimes for which an interception order may be obtained. AT&T supports these changes and suggests that consideration be given to including violations of 18 U.S.C. § 1030 (computer crimes) and 18 U.S.C. § 2511 (interception of electronic and oral communications) in the list of crimes.

The sixth major feature involves updating the basic provisions of the law with respect to the content of wiretap applications, the government's reporting obligations, the placement of certain mobile interception devices and the authorization of physical entry into a suspect's premises in order to install a bug or tap. The last mentioned provision provides that no order may require the participation of any individuals operating or employed by an electronic communications system in such physical entry. AT&T supports these portions of the bill.

As its seventh and last major feature, the bill would add new provisions prohibiting the use of pen registers and tracking devices without a court order. AT&T considers inadequate the wording of the subsection providing an exception for the use of a pen register by a provider of electronic communication services. The exception permits such use "relating to the operation, maintenance or testing of an electronic communication service." We urge that the exception be expanded to permit service providers to use pen registers in protecting against fraud or abuse of their services.

The new provisions concerning pen registers and tracking devices also contain a requirement that communications common carriers afford technical assistance necessary to accomplish the installation of pen registers or tracking devices when this is directed by a court order or upon the determination of an investigative or law enforcement officer that an emergency exists. In the latter case, a carrier is required to act at its peril since there is no way to determine whether the officer's assessment is justified. We urge that a provision be added to the bill making a good faith reliance on such an assessment a complete defense to any civil or criminal action brought against the carrier or any of its employees.

My comments today have necessarily been broad brush in nature. AT&T has recommended other important changes in H.R. 3378, and these are described in the detailed written analysis, dated October 25, 1985, which has been provided to the Subcommittee staff. In response to our analysis, and those of other entities, the staff has distributed for comment a draft revision of the bill dated November 11, 1985. AT&T's detailed comments on the draft are attached as an appendix to my written statement.

In conclusion, AT&T commends the Subcommittee's efforts to produce a sorely needed wiretap statute for the Information Age. We greatly appreciate the opportunity to participate in these early stages of legislation which would have a significant impact on our business. Needless to say, AT&T will continue to work with the Subcommittee staff which has been working diligently and tirelessly with our industry.

Mr. Chairman, that concludes my prepared statement and I would be happy to answer any questions at this time.

APPENDIX

JANUARY 30, 1986

## AT&T'S COMMENTS CONCERNING THE NOVEMBER 11, 1985 DRAFT REVISION OF H.R. 3378 PREPARED BY THE STAFF OF THE HOUSE SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE

The November 11, 1985 draft makes substantial improvements in the existing bill. The following comments concern matters that AT&T believes still require attention.

Section 101(a) - Draft p. 2

One of the cornerstones of the bill is the prohibition of the interception of electronic communications. As amended by Sec. 101(a)(2) of the bill, the definition of "intercept" in 18 U.S.C. § 2510(4) would be as follows:

> (4) "intercept" means interception of the contents of any electronic or oral communication through the use of any electronic, mechanical, or other device.

This involves the definition of a term with a derivation of the same term. "Interception" should be replaced with a series of words that would include as a minimum: acquisition, reception, copying and recording. Moreover, we believe that the definition should be revised to cover the interception of even part of a communication. Finally, the word "contents" should be deleted because the person who intercepts a digital message and leaves its decoding to another would not be intercepting the "contents" as defined in 18 U.S.C. § 2510(8).

Section 101(a) - Draft p. 2

It is unclear why H.R. 3378 deletes the word "existence" from the definition of "contents" in 18 U.S.C. § 2510. We pointed out in our October 25, 1985 comments that this deletion would create a divergence from the language of Communications Act Section 705. The November 11 draft revision of H.R. 3378 would prevent such divergence by deleting "existence" from Section 705 as well. However, doing so would weaken Section 705 by permitting carriers to disclose at will any available information concerning the date of and parties to an interstate or foreign communication, whether the information is in the form of billing records or otherwise. In contrast, Section 102(b) of H.R. 3378 would have the effect of narrowing the latitude allowed to carriers by Section 705, which permits carriers to disclose even the contents of a communication if they receive a subpoena or demand of other lawful authority. Section 102(b) would accomplish such narrowing by prohibiting electronic service providers from disclosing their records concerning a communication to the government in the absence of a court order. It is more in keeping with the spirit of H.R. 3378 to leave "existence" in Section 705 even though the bill deletes the word from the wiretap law's definition of "contents." The two statutes differ fundamentally in any event since Section 705 extends to non-intercepted communications that are beyond the scope of the wiretap law.

Section 101(a) - Draft p. 2

We believe that the bill requires a definition of "electronic communication system" to ensure that computers are covered by Section 102(a)'s proscription of the willful, unauthorized obtaining or altering of electronic communications stored in electronic communication systems. Our suggested definition of "electronic communication system" would be "any means of transmitting, receiving, processing, storing, retrieving or retransmitting electronic communications."

Section 101(b) - Draft pp. 3, 4

The bill carves out a number of exceptions to the prohibition of the interception of electronic communications. The first such exception permits the interception "of an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public." The broadness of this exception could deny protection to systems whose communications are readily susceptible to, but not intended for, interception by the public. We propose that the following phrase be added to the exception: "and the public is intended as the recipient of or participant in such communications." We also propose the addition of an exception to allow the release of call-tracing results to other electronic service providers and/or law enforcement officers as required by the circumstances of emergency, life threatening, harassing or fraudulent communications.

The new exceptions to the prohibition against interception should also expressly permit the "disclosure and use" of the information obtained. This would be consistent with the wording of existing exceptions contained in 18 U.S.C. § 2511(2)(a)(1) and (2)(b).

A revision on page 3 of the draft would permit the interception of electronic communications if it were done within the context of "conducting lawfully authorized intelligence activities in the normal course of such person's official duties." As frequent public debate in recent years had made clear, there is often disagreement within the government on the permissible scope of intelligence activities. Furthermore, a broad interpretation of "intelligence activities" would make the exception available to numerous agencies. This exception may therefore equate, as a practical matter, to a government carte blanche to circumvent the privacy protections intended by the bill.

Page 4 of the draft contains language permitting the use of pen registers to record the fact that an electronic communication was "completed." "Initiated" would be a better term. In the case of a telephone call, which is one type of electronic communication, there is no completion unless the called party answers.

Section 101(c) - Draft p. 4

The substitution of "electronic" for "wire" seems inappropriate in the case of the first use of "wire" in 18 U.S.C. § 2511(1)(b)(i). In that case, wire is used not as a modifier but only as a noun.

It appears that "of such communication" should be deleted from Section 2511(2)(a)(i).

Section 101(c) - Draft p. 5

The prohibition of 18 U.S.C. § 2512 of the mailing, distribution, advertising, etc. of intercept devices needs to be expanded to cover schemes to intercept electronic communications (e.g., plans and specifications for building and installing a wiretap).

Consideration should be given to adding to line 9 on page 5 "Section 2510(5)(a)." If this change is made, Section 2510(10) could be reworded to state that a provider of electronic communication service shall include a common carrier under 47 U.S.C. § 153(h).

Section 2511(1)(b) should be amended by the insertion of "electronic or" before "oral."

Section 102(a) - Draft p. 6

Changes are made in the prohibition of unauthorized accessing of electronic communication or the obtaining or altering of stored data. As revised, this important section continues to be confusing and fails to prohibit denials of service and the obtaining or altering of portions of stored communications. Moreover, it does not require that authorizing users be themselves authorized and acting within the scope of their authorization. Inserting the phrase "with respect to an electronic communication" seems inconsistent with the objective of reaching hackers who alter software. Our version would read:

> (3) Unless authorized by the person or entity providing an electronic communication service or by a user of that service acting within the scope of authority granted by such person or entity, and except as otherwise authorized in section 2516 of this title, whoever (i) willfully accesses an electronic communication system through which such service is provided or willfully exceeds an authorization to access that electronic communication service and (ii) obtains, alters, or interrupts or prevents access to, an electronic communication, in whole or in part, while the communication is stored in the system shall --

Section 102(a) - Draft p. 7

The bill prohibits, with specified exceptions, a provider of electronic communications service from divulging the "contents" of any communication carried over the service. The last exception substantially emasculates the prohibition by permitting disclosure by the provider "for a business activity related to a service provided by the provider of the electronic communication service to a user of the electronic communication service." [Emphasis supplied.] This may be tantamount to permitting any disclosures the provider chooses to make in the ordinary course of its business. The exception should be restricted to permitting disclosure only to an authorized originator or the intended recipient(s) of the communication or their agents.

Section 102(b) - Draft pp. 8, 9

Two additional exceptions should be added to the prohibition against disclosing certain electronic service provider records to governmental authority:

a) communications constituting an abuse of service or other illegal act (e.g., obscene calls, theft of communication service, computer abuse).

b) communications indicating a threat to life or property (e.g., a missing child calls for assistance or an elderly person collapses while talking to an operator).

We also suggest that exception (C) on page 9 be clarified by revising it to read as follows:

(C) pursuant to a court order under a statute specifically authorizing such an order, provided that notice of the order has been given by the governmental authority to the persons who are the object of the investigation.

The service provider should not be burdened with a court imposed obligation to give such notice.

Section 103 - Draft p. 9

Civil damages should be available when one's stored electronic communication is obtained, altered and when one's access to it is interrupted or prevented. (See suggested AT&T wording for Section 102(a) of the bill.)

Section 105 - Draft p. 11

We suggest that consideration be given to adding to the list of crimes: violations of 18 U.S.C. § 1030 (computer crimes) and 18 U.S.C. § 2511 (interception of electronic and oral communications).

Section 201 - Draft p. 16

The word "initiated" should be substituted for "completed" on line 10. (See similar suggestion on Section 101(b), Draft p. 4.)

Section 201 - Draft p. 20

The revisions on page 20 contain the gratuitous provision that a service provider "is not required to make such disclosure [of the use of a pen register] at any time." This language could be used in arguing that by implication there is a legal obligation for the service provider to eventually give such notice in cases where a statute does not excuse it. We recommend that the language be deleted.

Section 201 - Draft p. 24

Section 3136(a) of the new chapter on pen registers and tracking devices requires the Judge to whom a pen register installation application has been made to cause notice to be served upon affected persons. This corresponds with the notice requirement of 18 U.S.C. Sec. 2518(8)(d). AT&T strongly believes both sections must be clarified to indicate that the notice is to be given by the person or entity who applied for the order. This is the approach mandated by the Right to Financial Privacy Act. See 12 U.S.C. §§ 3405 and 3406.

Section 201 - Draft p. 25

The use of the word "inventory" on lines 11 and 13 is inconsistent with its deletion from Draft page 24, line 14.

Section 201 - Draft p. 27

Lines 12 and 13 appear to be missing a word. We suggest that the "s" be dropped from "registers" and "devices" and that "activity" be inserted after "device."

Mr. KASTENMEIER. Thank you very much for your brief but very informative statement, Mr. Amick. We will proceed, however, with Mr. Kelly and then have perhaps questions of you both.

Mr. Kelly.

Mr. KELLY. Thank you, Mr. Chairman.

Mr. Chairman and members of the subcommittee:

My name is John W. Kelly, Jr. I am an attorney with Southwestern Bell Telephone Co. and I am appearing before this committee on its behalf and on behalf of its parent company, Southwestern Bell Corp. concerning H.R. 3378, the Electronic Communications Privacy Act of 1985.

Southwestern Bell Corp. was formed during the reorganization of the former Bell system pursuant to judicial decree. Southwestern Bell Corp.'s subsidiaries include Southwestern Bell Telephone Co. and Southwestern Bell Mobile Systems, Inc.

Southwestern Bell Telephone Co. provides exchange, exchange access, and information access telecommunication services to its subscribers in the States of Missouri, Kansas, Arkansas, Oklahoma, and Texas.

Southwestern Bell Mobile Systems also provides services in these same five States involving cellular mobile telephone service.

Both companies under current law are communications common carriers and under the bill you are now considering would be classified as electronic communications providers. In either case, these firms are in the business of providing communications services to the public and support the intent of the proposed legislation as necessary and desirable in advancing the protections afforded by law to all forms of electronic communications.

Southwestern Bell has always stressed the singular importance of the privacy of our customers' communications. Our commitment to the protection of that privacy has not diminished because of the reorganization of the former Bell system.

We continue to believe that telecommunications users have an inherent right to the privacy of their communications—whether spoken or in the data transmission form—and regardless of the identify of the carrier who is providing service to that consumer or the technology used to provide such service.

The statute which H.R. 3378 would amend was enacted as a part of the Omnibus Crime Control and Safe Streets Act of 1968. In pertinent part, that legislation codified the protections afforded to telephone conversations and the procedures necessary for court authorized interception of those communications.

The 1968 legislation was appropriate for its time as to the state of the then current technology, the types of information which were transmitted, and the structure and regulation of the telecommunications industry.

The 1968 legislation is not, however, adequate almost two decades later for a number of reasons. Principal among these are: One, the dramatic changes in the structure of the telecommunications industry; two, the changing uses of the telecommunications services by the consuming public, both residential and business; and three, the constant and pervasive changes in the telecommunications technology.

In combination, these changes have diluted the protections of the 1968 statute. By the same token, these deficiencies would, in our view, be cured by the proposed legislation. A brief examination of these areas is appropriate.

Prior to 1968, telecommunications services were provided almost exclusively by communications common carriers which were franchised to provide local service and which provided long distance service in partnership with one another. Almost without exception, these carriers were not subject to competition.

In contrast, there is almost no aspect of telecommunications, or the broader field of electronic communications, which today is not competitive, with multiple suppliers capable and willing to provide alternatives to the once sole supplier.

H.R. 3378 recognizes this change in industry structure and extends the protections and privileges established by the 1968 law to all providers of the electronic communications services. Such a change is both necessary and appropriate—necessary to reflect the multiplicity of providers of electronic communications and appropriate to secure the same degree of protection to a consumer, regardless of his or her choice of vendor. The thing to be protected here is the privacy of communication, regardless of the identity of the carrier.

In 1968, the vast majority of all telephone communications were by the spoken word. That spoken word was protected from the unauthorized interception by the legislation passed in that year. By today's standards, computers were in their infancy and communication between computers was infrequent and unsophisticated. Given the state of the art and the usage of that art, it is not surprising that the 1968 law did not protect data transmissions from unauthorized interception.

Today, of course, the situation has changed dramatically. Data transmissions of all kinds are made by the thousands each day within a city or across the country. Data processing and the need for data transmission have increased substantially.

During the period 1972 through 1985, the growth rate in shipments of data processing equipment alone averaged approximately 17 percent annually versus an approximate 9-percent growth rate in telephone equipment, and an approximate 4-percent growth in gross national product.

For purposes of this legislation, it is not necessary to inquire into the causes of such a dramatic growth in data transmission. The fact is that modern American industry transmits highly confidential data in bulk on a daily basis and, in all probability, could not efficiently operate in any other manner. The data transmitted by such means is equally deserving, with voice communications, of protection against unauthorized interception.

H.R. 3378 achieves this goal by its redefinition of the term "interception" and thus resolves a problem which has existed since the passage of the 1968 legislation.

It would be an understatement to observe that the electronic communications industry has experienced significant technological advances in the past 20 years. Some of these changes include the development of transmission media other than wire and radio, as defined in the 1968 statute.

The bill now before you, Mr. Chairman, broadens the scope of protection against unauthorized interception so that all electronic communications are protected, without regard to the medium by which they are transmitted.

As noted before, that which is deserving of protection is the communication itself and such protection should not be diluted or foreclosed because of the choice of transmission media.

The 1968 statute provided certain limited exceptions to the otherwise comprehensive prohibition against interceptions of telephonic communications. Those exceptions permitted communications common carriers to engage in limited forms of interception when such activity was inherent in the rendition of service or necessary to protect the telephone company's rights or property.

As we understand the bill, these exceptions are continued for both telephone companies and other providers of electronic communications without material substantive change. The bill does, in title II, treat pen registers separately from intercepting equipment. That treatment retains, however, the authority for electronic communications providers to employ pen registers for both operational, testing and maintenance purposes and in abuse of service cases.

These exceptions are limited in nature, parallel those already in the law and should be retained in the bill.

Since the introduction of H.R. 3378, Southwestern Bell has received a November 11, 1985, proposed revision of the bill which is currently pending in the House and the Senate.

The modifications contained in the November 11 proposed revision resolve many of the concerns which have been previously discussed by Southwestern Bell with members of the subcommittee staff. As modified in that proposed revision, Southwestern Bell Corp. supports the passage of the Electronic Communications Privacy Act of 1985.

We appreciate the opportunity to appear before the subcommittee, Mr. Chairman, and to work with members of the committee staff regarding the provisions of this bill.

If the members of the committee have any questions, I would be pleased to respond to them at this time. Thank you.

[The statement of Mr. Kelly follows:]

# UNITED STATES HOUSE OF REPRESENTATIVES

## COMMITTEE ON THE JUDICIARY
## SUBCOMMITTEE ON COURT, CIVIL LIBERTIES, AND THE ADMINISTRATION OF JUSTICE

## STATEMENT OF
## JOHN W. KELLY, JR., ATTORNEY
## SOUTHWESTERN BELL TELEPHONE COMPANY
## REGARDING H.R. 3378, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985

## JANUARY 30, 1986

Mr. Chairman and members of the Subcommittee, my name is John W. Kelly, Jr. I am an attorney with Southwestern Bell Telephone Company and am appearing before this Committee on its behalf and on behalf of its parent company, Southwestern Bell Corporation, concerning H.R. 3378, the "Electronic Communications Privacy Act of 1985."

Southwestern Bell Corporation was formed during the reorganization of the former Bell System pursuant to judicial decree. Southwestern Bell Corporation's subsidiaries include Southwestern Bell Telephone Company and

Southwestern Bell Mobile Systems, Inc. Southwestern Bell Telephone Company provides exchange and exchange/information access telecommunication service to its subscribers in Missouri, Kansas, Arkansas, Oklahoma and Texas. Southwestern Bell Mobile Systems provides cellular mobile telephone service in the same five-state area.

Both companies are, under current law, communications common carriers and, under the Bill you are now considering, would be classified as electronic communications providers. In either case, these firms are in the business of providing communications services to the public and support the intent of the proposed legislation as necessary and desirable in advancing the protections afforded by law to all forms of electronic communications.

Southwestern Bell has always stressed the singular importance of the privacy of our customers' communications. Our commitment to the protection of that privacy has not diminished because of the reorganization of the former Bell System. We continue to believe that telecommunications users have an inherent right to the privacy of their communications--whether spoken or in data transmission form--and regardless of the identity of the carrier who is providing service to that consumer or the technology used to provide such service.

The statute which H.R. 3378 would amend was enacted as a part of the Omnibus Crime Control and Safe Streets Act of 1968. In pertinent part, that legislation codified the protections afforded to telephone conversations and the procedures necessary for Court authorized interception of those communications. The 1968 legislation was appropriate for its time, as to the state of then current technology, the types of information which were transmitted, and the structure and regulation of the telecommunications industry.

The 1968 legislation is not, however, adequate almost two decades later for a number of reasons. Principal among these are (1) the dramatic changes in the structure of the telecommunications industry; (2) the changing uses of telecommunications services by the consuming public, both residential and business; and (3) the constant and pervasive changes in telecommunications technology. In combination, these changes have diluted the protections of the 1968 statute. By the same token, these deficiencies would, in our view, be cured by the proposed legislation. A brief examination of these areas is appropriate.

1) Changes in Industry Structure.

Prior to 1968, telecommunications services were provided almost exclusively by communications common carriers which were franchised to provide local service and which provided long distance service in partnership with one another. Almost without exception, these carriers were not subject to competition. In contrast, there is almost no aspect of telecommunications (or the broader field of electronic communications) which today is not competitive, with multiple suppliers capable and willing to provide an alternative to the once sole supplier.

H.R. 3378 recognizes this change in industry structure and extends the protections and privileges established by the 1968 law to all providers of electronic communications services. Such a change is both necessary and appropriate--necessary to reflect the multiplicity of providers of electronic communications and appropriate to secure the same degree of protection to a consumer, regardless of his or her choice of vendor. The thing to be protected here is the privacy of communication, regardless of the identity of the carrier.

2) Changes in Consumers' Uses of Communication.

In 1968, the vast majority of all telephone communications were by the spoken word. That spoken word was protected from unauthorized interception by the legislation posed in that year. By today's standards, computers were in their infancy and communication between computers was infrequent and unsophisticated. Given the state of the art and the usage of that art, it is not surprising that the 1968 law did not protect data transmissions from unauthorized interception.

Today, of course, the situation has changed dramatically. Data transmissions of all kinds are made by the thousands each day within a city or across the country. Data processing and the need for data transmission have increased substantially. During the period 1972 through

1985, the growth rate in shipments of data processing equipment alone averaged approximately 17 percent annually versus an approximate 9 percent growth rate in telephone equipment (and an approximate 4 percent growth in gross national product). For purposes of this legislation, it is not necessary to inquire into the causes of such a dramatic growth in data transmission. The fact is that modern American industry transmits highly confidential data in bulk on a daily basis and, in all probability, could not efficiently operate in any other manner. The data transmitted by such means is equally deserving, with voice communications, of protection against unauthorized interception. H.R. 3378 achieves this goal by its redefinition of the term "interception" and thus resolves a problem which has existed since the passage of the 1968 legislation.

3) Changes in Technology.

It would be an understatement to observe that the electronic communications industry has experienced significant technological advances in the past 20 years. Some of these changes include the development of transmission media other than wire and radio, as defined in the 1968 statute. The Bill now before you, Mr. Chairman, broadens the scope of protection against unauthorized interception so that all electronic communications are protected, without regard to the medium by which they are transmitted. Such a change is clearly desirable and in the public interest. As we noted before, that which is deserving of protection is the communication itself and such protection should not be diluted or foreclosed because of the choice of transmission media.

A simple example, perhaps close to home, should illustrate this point. You can today place a telephone call from your home by means of a traditional telephone instrument and your communication would be protected under existing law. Should that protection be any less because you choose (perhaps only for convenience) to place the call by means of a "cordless telephone" or because you place that same call from a cellular telephone located in your automobile? Southwestern Bell Corporation believes that all three of these communications are entitled to the same degree of protection and we view H.R. 3378 as affording that protection, both for current technology and for any foreseeable future technology involving a total or partial use of wire, radio, electromagnetic or photoelectric transmission systems.

The 1968 statute provided certain limited exceptions to the otherwise comprehensive prohibition against interceptions of telephonic communications. Those exceptions permitted communications common carriers to engage in limited forms of interception when such activity was inherent in the rendition of service or necessary to protect the telephone company's rights or property. Typically, a telephone company's activity in this area took the form of service testing and monitoring, call tracing activity in abusive or harassing call cases, and limited interceptions in toll fraud cases.

As we understand the Bill, these exceptions are continued--for both telephone companies and other providers of electronic communications--without material substantive change. The Bill does, in Title II, treat pen registers separately from intercepting equipment. That treatment retains, however, the authority for electronic communications providers to employ pen registers for both operational, testing and maintenance purposes and in abuse of service cases. The latter category would, in our view, cover both the harassing call situations and our investigation of toll fraud. These exceptions are limited in nature, parallel those already in the law (18 U.S.C. § 2511(2)) relating to the interception of oral communications, and should be retained in the Bill.

Since the introduction of H.R. 3378, Southwestern Bell has received a November 11, 1985, proposed revision of the Bill which is currently pending in the House and Senate. The modifications contained in the November 11 proposed revision resolve many of the concerns which have been previously discussed by Southwestern Bell with members of the subcommittee staff. As modified in that proposed revision, Southwestern Bell Corporation supports passage of the Electronic Communications Privacy Act of 1985.

We appreciate the opportunity to appear before the subcommittee, Mr. Chairman, and to work with members of the committee staff regarding the provisions of this Bill. If members of the committee have any questions, I would be pleased to respond to them at this time.

Mr. **Kastenmeier.** Thank you, Mr. Kelly, for that very informative statement.

To your knowledge, would other regional telephone companies likely have similar views to those expressed by you for Southwestern Bell Telephone? There is no reason they would have different views, would they?

Mr. **Kelly.** Mr. Chairman, I would have no reason to believe that they would have different views.

Mr. **Kastenmeier.** Obviously, the 1968 law written as it was, was just to a very limited extent able to anticipate either a corporate structure, corporate reorganization, customer uses and new technology in that point in time, now nearly 18 years ago.

Within the next few years, many phone companies will doubtless offer a wide array of communications technologies potentially to customers. I would like to solicit your view as to, let's say within the next 10 years, what percentage of your networks you estimate will be devoted to traditional phone calls as we have known in the past and know at the present time as opposed to, let's say, data, video, or other nonvoice communications.

Mr. Amick, do you have any view on that? Do you have a sense of what change might take place within the next 10 years?

Mr. **Amick.** Mr. Chairman, in 1976, virtually all voice transmission was what we were familiar with the traditional telephone call. Computer-to-computer transmission was in its infancy and could not be entertained in the legislation.

Today, virtually all long distance is digitized and to determine the percentage of voice versus data versus video is becoming less material as it is all interspersed in a digital manner.

Today approximately 70 percent of all information transmissions, be they data or voice, are digitized. It is estimated that by 1990, 90 percent will be digitized. The future ability to differentiate between voice, data, video, and any other services that may appear over the technological horizon is impossible to determine at this time.

Mr. **Kastenmeier.** So, in a nutshell we had better expect change because change is going to take place with reference to dependence on new technologies as opposed to traditional transmissions?

Mr. **Amick.** Yes, sir.

Mr. **Kastenmeier.** As you have pointed out, there are now more common carriers and more competitors—Mr. Kelly made that point. What percentage of electronic communications currently are carried over noncommon carriers, that is, electronic mail, PBX's, and the like. What might that percentage be in the future? What is the situation today and what change might you contemplate in the future in that respect, either of you?

Mr. **Kelly.** Mr. Chairman, I will be happy to address that question.

We are at a disadvantage in terms of quantifying that percentage of communications of traffic because many of the noncommon carriers that do carry traffic, we have no way of compelling disclosure of the amount of traffic that they do carry.

Mr. **Kastenmeier.** I appreciate that but could you characterize it by a small amount today, but a growing percentage? Could you contemplate, at least could you give us some sort of guideline, if that or some other characterization might be accurate?

Mr. **Kelly**. I think what you say, Mr. Chairman, is definitely the situation today. It is a growing experience of noncommon carriers wanting to carry more traffic that was previously carried by the regulated common carrier. You have your shared tenant service providers, you have your private networks that are being created—all of which are continuing to build their own networks. Numerically it would be very difficult to try to put a percentage on it except to be very comfortable in predicting that that percentage of traffic will increase in the future being carried by noncommon carriers.

Mr. **Kastenmeier**. At least to the question contemplating this legislation, should all electronic communications providers be protected against interception regardless of size, in your view?

Mr. **Kelly**. I think the primary focus, Mr. Chairman, is the user of the communications. Certainly I would support that all communications by the user, be it provided by a small provider of electronic communications or a large one, should be protected—the size of the provider should not make any difference.

Mr. **Kastenmeier**. Yes; I think some people prefer to identify the problem not in terms of the providers but either in terms of the users or in terms of the service itself, the technology rather than who provides it.

One of the things we must wonder about is whether it is realistic to expect, at least from a criminal law standpoint, enforcement of any such law that might provide protection to individuals, with explosion, literally, of electronic communications. Might we have an enormous problem in enforcement in the future, if not today? Mr. Amick?

Mr. **Amick**. Mr. Chairman, the purpose of the legislation, of course, is to act as a deterrent and to provide appropriate penalties for those who violate that deterrence.

Yes; there would, obviously, be an increase in the violations, but I think those violations must be prosecuted in accordance with the law. It is only through the prosecution of the statutes that deterrence is effective.

Mr. **Kelly**. Mr. Chairman, may I address that question?

Mr. **Kastenmeier**. Yes, Mr. Kelly.

Mr. **Kelly**. From my standpoint, it may very well be more cumbersome for the law enforcement agencies to deal with the multiple and competitive electronic communications providers. But I think that is the price that one pays for shifting the industry to a competitive one. I don't believe that it is these amendments that would cause necessarily the FBI to have to experience more time and effort in enforcing the law.

Mr. **Kastenmeier**. Thank you for those comments. I have a couple more questions but I think I ought to yield to my colleagues at this time. The gentleman from California, Mr. Moorhead.

Mr. **Moorhead**. Thank you, Mr. Chairman.

Mr. Kelly, a piece of legislation has been introduced in the Congress and has been referred to the Energy and Commerce Committee, the Telecommunications Subcommittee, which would release regional Bell operating companies, including yours, from many of the restrictions that were imposed at the time of divestiture.

If such restrictions were removed there would in time be significantly more data transmissions between homes and banks and stores and other data bases. Will this bill offer the type of protection for individuals that is vital in this kind of expanded coverage?

Mr. **Kelly**. Mr. Moorhead, we, of course, endorse the proposal to lift those restrictions, lines of business restrictions. I believe that as the bill is proposed it would protect the users' privacy of communications of the types of information that would be communicated on the network.

Mr. **Moorhead**. Do you have an opinion on that also?

Mr. **Amick**. Mr. Moorhead, regardless of the carrier or the nature of the service being provided, we feel it imperative that legislation of this nature be enacted to provide the protections that are going to be required in tomorrow's technology.

Mr. **Moorhead**. Later on this morning we are going to receive testimony from Mr. Richard Colgan who represents the Association of North American Radio Clubs. In his written testimony he suggests that with regard to land, mobile, and other radio services the presence or absence of encryption should be the test as to whether the system provider and the user expect privacy.

What is your view as to whether or not encryption or the lack thereof should be the determining factor in whether a given radio service is protected?

Mr. **Amick**. Our position would be that subscribers to services not intended for broadcast to the general public, are entitled to an expectation of privacy regardless of the encryption devices used. Encryption would be an added—user supplied—feature to better protect an information transmission. Encryption should not necessarily be the threshold to any prosecutive efforts.

Mr. **Moorhead**. Mr. Kelly, do you have an opinion on that?

Mr. **Kelly**. Yes, sir.

Our position is that the law, as amended, would have sufficient penalties as a deterrent from interception of those communications that it may be premature to consider encryption at this point in time. Obviously, to involve encryption would include the cost of doing that. I am afraid I can't quantify that at this time but there certainly would be cost considerations. But there are sufficient penalties to deter that kind of activity, intentional interception, that is in place in the bill.

Mr. **Moorhead**. Thank you both very much.

Mr. **Kelly**. Thank you.

Mr. **Kastenmeier**. The gentleman from North Carolina.

Mr. **Coble**. You and Mr. Moorhead, I think, have covered what I was going to comment on.

I would like to express my thanks, Mr. Chairman, to the two witnesses. Oftentimes we have witnesses who read 25 to 50 pages and lull me to sleep. Neither of you did that and I thank you for your precise presentation. Thank you.

Mr. **Amick**. You are welcome.

Mr. **Kastenmeier**. The gentleman from Georgia, Mr. Swindall.

Mr. **Swindall**. No questions, thank you.

Mr. **Kastenmeier**. I have just one or two questions left.

As I recall your testimony, Mr. Kelly, you indicated you were satisfied with the changes made, the definition of intercept or interception, but indeed, Mr. Amick indicated that the term intercept or interception should be replaced with a somewhat different terminology in terms of what is intended. Having heard him make those remarks, I wonder, Mr. Kelly, what your view is. Do you agree with Mr. Amick or are you content with interception as it appears in the bill?

Mr. KELLY. I think, Mr. Chairman, that Mr. Amick has some very good points in connection with the definition of interception. His proposed modifications to interception I think would be an enhancement to the current proposed amendment. While we were satisfied with your definition, I think the wisdom of sharing ideas here has shown that others have some improvements that they may very well suggest.

Mr. KASTENMEIER. Mr. Amick, you indicated in your testimony that data and video transmissions are indistinguishable from voice transmissions, I believe. Could you elaborate? Could you explain what you mean by that?

Mr. AMICK. In the data flow through our long-distance circuitry, the voice modulated frequency is converted to a series of bits, merely on or off, one-two, one-two, one-two. As they go through the system on the other end they are put back together again into voice or video or data. As they are going through that system they are indistinguishable. I think the definition that I have heard is that a computer bit, is a bit, is a bit—unintelligible.

Mr. KASTENMEIER. I have another question or two which I am not going to burden this particular hearing with because it is a little more technical. If you do not object, I would like to present a question or two that I still have to you, inviting you to communicate by letter and we can add that to your testimony.

Mr. AMICK. Surely.

Mr. KASTENMEIER. I would like to yield to the gentleman from California, Mr. Berman.

Mr. BERMAN. No questions, Mr. Chairman.

Mr. KASTENMEIER. Let me ask—you have answered a very important question on encryption—what your further views are in terms of the collision of interests with respect to the use of radio or other similar new technologies with respect to the use for communications such as telephone as provided in the past, computers, and so forth. Are those who have traditionally relied upon freedom of the radio waves being out there to intercept virtually without restriction. Is there any, in your view, reasonable policy, a way policywise, to resolve that conflict in expectations—expectation on the user for privacy, the expectation on the, let's say, radio operator, to be freely able to pick up signals. Is there an expectation of privacy? Mr. Kelly.

Mr. KELLY. Mr. Chairman, I think the question is a very challenging question. I am not sure I have an answer for it. I have some observations. I think we still have to consider the bottom line here of protection of conversations, communications, be it over whatever medium. If we are into the radio cellular communications, this is the new consideration we have to address, that the users of cellular expect privacy in their two-way communications, while at the same time, as you mentioned, radio users have enjoyed, for the most part, freedom of the airwaves. There has to be some accommodation there.

I think at this point in time whatever possible interception there may be, it is probably rather short, minute, and certainly not intentional. As we view the cellular business, customers who are using the phone go from one cell to another. So, it would be difficult for other parties to intercept that conversation continuously. Of course, we want to encourage privacy of that communication as much as possible.

I have rambled a little here. I am not sure I have really an answer to that. It is something I think we are going to have to continue to address. I am sure there is a way to make both parties satisfied in their use of whatever transmission or medium they choose to use.

Mr. KASTENMEIER. Thank you.

Mr. Amick, do you have any comment?

Mr. AMICK. I can only reinforce Mr. Kelly's statement. Our principle is that the users of our services, that are not intended for broadcast to the general public, should be afforded an expectation of privacy.

Mr. KASTENMEIER. If there are no further questions, the committee is grateful to you both for your appearance here this morning. This represents, as you have indicated in your testimony, a statement of your position. In addition you have indicated you have had an opportunity to work with the committee staff and others during the past number of months to offer comment and to participate in the preparation of legislation which could bring our laws up to date with respect to electronic communications. We are indebted to you both.

Mr. KELLY. Thank you.

Mr. AMICK. Thank you, Mr. Chairman.

Mr. KASTENMEIER. I would like to introduce our second and final panel this morning. On our final panel we have three witnesses. First, Mr. Perry Williams, who is corporate secretary and Washington area coordinator of the American Radio Relay League, National Association of Amateur Radio Operators.

Mr. Williams has been a ham radio operator since 1951, nearly 35 years. He has been with the league for more than 30 years.

Also, I would like to call forward at this time the person who will follow Mr. Williams, Mr. George Kuhnreich. Mr. Kuhnreich is vice president for corporate planning and governmental affairs for Tandy Corp., manufacturers and distributors of scanning and other radio equipment. Mr. Kuhnreich is an attorney and has been with Tandy since 1977.

Finally, we would like to greet Mr. Richard Colgan, executive secretary of the Association of North American Radio Clubs. Mr. Colgan is a shortwave radio listener, and has been a radio enthusiast since 1959.

Gentlemen, again, we have your written statements. They will be, without objection, made part of the record, and you may proceed as you wish. I will call on Mr. Williams first. Mr. Williams.

## TESTIMONY OF PERRY F. WILLIAMS, SECRETARY, THE AMERICAN RADIO RELAY LEAGUE, INC.; GEORGE A. KUHNREICH, VICE PRESIDENT, CORPORATE PLANNING AND GOVERNMENTAL AFFAIRS, TANDY CORP., AND RICHARD T. COLGAN, EXECUTIVE SECRETARY, ASSOCIATION OF NORTH AMERICAN RADIO CLUBS

Mr. WILLIAMS. Mr. Chairman, distinguished representatives, ladies and gentlemen:

Thank you for inviting me to speak on behalf of the Nation's 416,000 licensed radio amateurs. Our written testimony briefly sketches what the amateur service is, and the public services it performs.

The testimony establishes that there is no expectation of privacy in amateur radio. This opinion was supported by the Congress as recently as 1982 in Public Law 97-259 when it amended section 605, now 705, of the Communications Act.

Wisely, the proposed Electronics Communications Privacy Act continues to exempt amateur transmissions. If report language makes it clear that amateur communications are exempt at all times even when the radios are connected to telephone or data networks, our basic concerns are met.

However, there is one more problem not fully developed in our text, similar to the concerns being expressed by the community of listeners here today—the tradition, nearly 75 years old, that amateurs are free to monitor any radio transmissions whose waves pass over their receivers. This concept was stated in the 62d Congress as it reported on bills to regulate radio communication in 1912.

To quote from that report: "The bill does not interfere in any way with the hearing of messages by amateurs at all times and places as they may elect." "Amateur" in that context was generic—it included listeners. This freedom is not just in the abstract. Amateurs need it to continue doing their public works.

When amateurs help the Forest Service fight brush fires in California they have to keep one ear on Forest Service frequencies.

When serving as tornado spotters—as 30,000 amateurs do—throughout the midsection of the country, they monitor weather service circuits.

Along the coasts of the country, amateurs helping the Coast Guard respond to boats in distress must listen on maritime frequences.

And when we help the Civil Air Patrol, we are monitoring aeronautical circuits.

So, the need for freedom to listen is still there and still in the public interest.

The checks and balances of section 705 tying "intercepting" to "divulging or using" seem to have served well for 7½ decades. Such a concept still is valid.

Thank you.

Mr. KASTENMEIER. Thank you very much, Mr. Williams.

[The statement of Mr. Williams follows:]

Before the
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES
AND THE ADMINISTRATION OF JUSTICE

of the

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES
Washington, D.C. 20515

Statement of

Larry E. Price, Ph.D.

President of The American Radio Relay League, Incorporated

on

Bill H.R. 3378--"The Electronic Communications Privacy Act of 1985"

Presented by
Perry F. Williams
Secretary of The American Radio Relay League ic.
Thursday, January 30, 1986

The American Radio Relay League, Incorporated is the national, non-profit organization representing the interests of the more than 400,000 amateur radio operators licensed in the United States by the Federal Communications Commission. The League is appreciative of the opportunity to submit to this Subcommittee the views and concerns of amateur radio operators relative to the instant proposed legislation.

The Amateur Radio Service is allocated various radio frequency bands for local, regional, national and worldwide communications. Such communications promote technical self-training and provide a unique ability to enhance international goodwill. More importantly, however, amateurs are expected to and do provide regular public service and emergency communications. In every major disaster, amateur radio operators provide communications where other facilities are destroyed or overtaxed. Most recently, following the earthquake in Mexico City, and the various hurricanes along the southern and east coasts of the United States, rescue efforts were coordinated via amateur radio and literally tens of thousands of health and welfare messages were exchanged by amateur radio links. Every day, amateur radio operators put armed services and government personnel in touch with their families in the United States when otherwise such communications would be impossible. Networks of amateurs who relay messages are responsible for obtaining medical supplies on short notice for people who would not survive without it. The Federal Communications Commission has termed such operation a "priceless public benefit." In addition, amateurs have developed networks of computer data banks known as "packet networks" accessed by, and linked together with, amateur radio stations. These provide extremely rapid and error-free computer communications.

Because there are more than one and one-half million radio amateurs operating worldwide, using the same bands of radio frequencies, no one communicating via amateur radio or via amateur radio frequencies has any reasonable expectation of privacy. United States v. Sugden, 226 F.2d 281 (9th Cir. 1955) (dictum), aff'd 351 U.S. 916 (1956). A reasonable person would not expect that words uttered over an amateur radio frequency would be heard only by those few individuals for whom the communication was specifically intended. United States v. Hill, 50 Pike & Fischer Radio Regulations 2d 1331 (U.S. Court of Appeals, 1st Cir. 1982). All amateur radio operators may use any of the channels allocated to the Service (subject to transmitting restrictions based on operator license class). Thus, those utilizing amateur radio frequencies do not enjoy any expectation of privacy. See H.R. Conf. Report No. 97-765, 97th Cong., 2d Sess. at 60 (1982); reprinted in 1982 U.S. Code Cong. & Ad. News 2261. In 1982, Congress amended then §605 (now §705) of the Communications Act, 47 U.S.C., so as to clarify the absence of any expectation of privacy in connection with amateur communications and thus the exemption from the reception and disclosure restrictions of 47 U.S.C. §705.

The creation of an expectation of privacy in amateur radio is further unnecessary and antithetical to the nature of the Service. The FCC Rules and Regulations governing the Amateur Radio Service (Title 47, CFR Part 97) prohibit business communications (See §97.110); prohibit the transmission of messages for hire, or for material compensation, direct or indirect, paid or promised (See §97.112); and prohibit third-party traffic involving material compensation to any person and traffic consisting of business communications on behalf of any party (See §97.114). The Radio Regulations (Geneva 1982) require that transmissions between amateur radio stations of different countries, when permitted, must be limited to "messages of a technical nature relating to tests, and to remarks of a personal character for which, by reason of their unimportance, recourse to the public telecommunications service is not justified." Section 97.111 of the FCC Rules reiterates this treaty requirement. There are, of course, exceptions to these prohibitions relating to disaster communications. The instant Bill, however, wisely also contemplates exempting disaster communications from privacy considerations. Accordingly, no legitimate amateur radio communications demand the protection afforded by the Privacy Act.

The instant Bill would, inter alia, vastly expand the present wiretap and oral communication interception prohibitions of Chapter 119 of Title 18, United States Code, to include "electronic communications" generally. The Bill does, however, contain a provision which purportedly exempts amateur radio communications from the general prohibition of electronic communication interception. Subsection 2511(2)(g) would read, in part, as follows:

> (g) It shall not be unlawful under this chapter for any person --
>
> * * * * *
>
> (ii) to intercept any electronic communication which is transmitted --
>
> * * * * *
>
> (III) by an amateur radio station operator or by a citizens band radio operator; . . .

In addition to the above, there are other provisions within Subsection 2511(2)(g) which could be construed to exempt amateur radio communications from the proscriptions of the Bill.

Provided that the specific exemption for amateur radio communications remains in the Bill and that the same is construed and intended to apply to all forms of communication by, between and among licensed amateur stations on frequencies allocated to the Amateur Radio Service, then the League's most basic concerns are essentially satisfied. Discussions with Subcommittee staff, however, yield concerns that the Bill may be interpreted to preclude or limit the ability of amateurs to monitor those amateur radio communications involving telephone interconnect, in which one party to the amateur communications speaks and listens through a telephone line "patched" to an amateur radio transmitter and receiver. It is via these "phone patches" that amateurs put overseas servicemen in touch with their families, notify police, fire and ambulance services of emergencies, notify the Coast Guard of ships in distress, and initiate and terminate health and welfare message traffic. Phone patching has been an integral part of amateur radio emergency and public service communications since at least the Korean War, when amateurs provided communications for wounded military personnel aboard hospital ships in the Far East. The propriety thereof has been acknowledged by the Federal Communications Commission. See Carter v. AT&T Co., 13 FCC 2d 420, 13 Pike & Fischer Radio Regulations 2d 597 (1968).

Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems, are certainly not those to which this "privacy of communications" legislation is aimed. It is thus respectfully requested that any report language to accompany this legislation clearly state that all amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Service are exempt from the electronic communications intercept prohibitions of the Bill. If in the opinion of the Subcommittee the present language of the Bill does not sufficiently exempt all amateur radio communications, then the same should be amended to include, for example, an exemption for electronic communications transmitted "on frequencies allocated to the Amateur Radio Service" or the like.

Finally, it should be noted that amateurs, in performing their public service functions, occasionally utilize communications of other services, such as NOAA weather broadcasts and the like. As such, many amateurs employ "scanner" receivers which are capable of receiving communications of many different radio services (including amateur VHF and UHF communications, typically). The use of, as an example, a multiband radio receiver by a licensed amateur should not subject the amateur to criminal prosecution or harassment in any fashion. Amateurs have legitimate reason to monitor frequencies outside the amateur bands. Many amateurs, for instance, are enrolled in the Military Affiliate Radio System and the Civil Air Patrol, which use frequencies assigned to the Department of Defense. Others are members of the Coast Guard Auxiliary using frequencies in the Maritime Service allocation. Some 30,000 amateurs are part of Skywarn, a system operated by the National Weather Service for tracking and warning of severe weather conditions, e.g., tornadoes; at times it may be required that they monitor Government frequencies in connection with this work. In short, there is legitimate reason for amateurs to have equipment which tunes beyond amateur bands. Amateurs must not be exposed to well-meaning but uninformed enforcement activities under the proposed Title 18 revisions. Overall, it would appear that the Bill does not contain sufficient exemptions for legitimate users of radio spectrum.

On behalf of the more than 400,000 amateur radio operators of the United States, I thank you very much for the opportunity to participate in this hearing.

Mr. **Kastenmeier**. Now I would like to call on Mr. George Kuhnreich. Mr. Kuhnreich.

Mr. **Kuhnreich**. Good morning, Mr. Chairman, members of the committee. We are very pleased to be here.

I am representing the Tandy Corp., which is the largest retailer of consumer electronic products in the United States with some 6,000 stores domestically located, and backed up by 31 factories in the United States.

We are both a manufacturer and a distributor of telephones and radio transmitting and receiving equipment, including cellular and cordless handsets, shortwave radio, and police and public safety ban scanners. As such, we have a vital interest in this legislation.

At the outset, Mr. Chairman, I would like to mention that we have submitted a detailed statement of our position to the committee which I would like to summarize very briefly.

H.R. 3378 is intended principally to afford privacy protection to those using communication technologies such as cellular radio or electronic mail that have emerged since adoption of the original Federal wiretapping and eavesdropping provision of the Omnibus Act.

Tandy supports the extension of privacy protection to cellular communications as well as to all forms of encrypted communications. Given the technology of the cellular industry, including the hands-off calls from cell to cell, the cellular telephone subscriber simply does not differentiate between cellular calls and conventional landline telephone calls. The subscriber thus perceives that, like wire communications, cellular calls are private and protected from interception.

As a practical matter, Tandy believes that extension of privacy protection to cellular communication will help ensure the continued growth and vitality of the cellular industry. Should protection be denied subscribers, cellular service could become less attractive vis-a-vis landline services. As the cellular industry is now in its infancy, denial of privacy coverage could well significantly impair the competitive viability of cellular technology. Tandy thus submits that the extension of privacy coverage of the cellular communications could well serve the dual goals of fostering competition among the communications services, and encouraging the utilization of the state-of-the-art technology.

Similarly, encrypted transmission are by the very act of encryptions converted to a form of private communications and should be accorded privacy accordingly.

The extension of the Omnibus Act protections to cellular and encrypted communication will conform existing statutes that are the public's perception and expectations.

Tandy's sole and limited concern with H.R. 3378 as drafted is that the bill may be overly inclusive and extend privacy protection to categories of communications in which there has never been any perception or expectation of privacy.

While amateur radio CB and police and public safety band communications are excluded from protection of H.R. 3378, the bill does extend privacy coverage, for example, to ship-to-shore communications. Unlike cellular communications, however, these messages traditionally have not been thought by the message centers to be subject of privacy protection.

As a blue water sailor, I can assure the committee that if I ever get myself in trouble and I am yelling "May Day," I would like everyone to hear it.

Tandy believes that perhaps inadvertent impact of H.R. 3378 on communications service to which there is no perception or expectation of privacy would be great. While the exact numbers are not available at this time, we estimate conservatively that there are over 350,000 amateur radio operators in the United States, each typically owning more than one receiver.

There are somewhere between 40 and 60 million CB's and walkie-talkies operational within the United States. In total, there are perhaps over 120 million receivers which potentially could be affected by H.R. 3378. Clearly, legislation with a potential for such enormous impact upon the populous and its accumulated investment warrants very careful consideration.

Mr. Chairman, I would be happy to answer any questions.

[The statement of Mr. Kuhnreich follows:]

# STATEMENT OF GEORGE A. KUHNREICH
Vice President for Corporate Planning
and Governmental Affairs

TANDY CORPORATION

On H.R. 3378, The Electronic
Communications Privacy Act of 1986

Before the House Judiciary Subcommittee On Courts,
Civil Liberties, and Administration of Justice

House Committee on the Judiciary

January 30, 1986

## Statement of George A. Kuhnreich Vice President for Corporate Planning and Governmental Affairs, Tandy Corporation

## On The Electronic Communications Privacy Act of 1986

Mr. Chairman and Distinguished Members of the Subcommittee:

My name is George A. Kuhnreich and I am Vice President for Corporate Planning and Governmental Affairs of Tandy Corporation ("Tandy"). I am pleased to have the opportunity to appear before you today to present the views of Tandy Corporation regarding H.R. 3378, a bill to amend the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Omnibus Act") (18 U.S.C. §2510 et. seq.) relating to interception of private communications through "wiretapping" and "eavesdropping". H.R. 3378 would extend the protection accorded such communications to encompass, with specified exceptions, messages transmitted via a wire, radio, electromagnetic, or photoelectric system that effects interstate or foreign commerce."

### I. Introduction and Summary

Among its business interests, Tandy is a manufacturer and distributor of both telephone and radio transmitting and receiving equipment -- e.g., cellular and cordless hand-sets, short-wave radios, citizen band radios ("CBs") and police and public safety band scanners. Indeed, through its 4,400 "Radio Shack", 450 "Radio Shack Computer Center" and 130 "Radio Shack Telephone Store" sales outlets, Tandy serves over 29 million American families, and is the largest retail distributor of consumer electronic products in the United States -- a position that it has acquired through its more than 65 years of service to the public. As the number one retailer in the industry, Tandy is necessarily attuned to the ever-changing needs and desires of the consuming public. Since H.R. 3378 would impact either directly or indirectly virtually all of the communications services in which electronic equipment is designed to operate, Tandy especially welcomes this opportunity to provide the Subcommittee with its perspective on the pending legislation.

Tandy agrees with Representatives Kastenmeier and Moorhead, and their Senate colleagues, Senators Mathias and Leahy, that the extraordinary developments in the telecommunications industry since 1968 have made obsolete the provisions in the Omnibus Act relating to privacy in communications.[1] The advent of new voice and data transmission facilities and services -- for example, "electronic mail", telecopying services and cellular telephony -- has, in fact, dramatically altered the personal and business communications environment. But, to date, there has been no accompanying evolution in the law to provide privacy protection for categories of communications that were not contemplated at the time of enactment of the Omnibus Act. Nevertheless, in order to foster the development of emerging communications industries, such protection may be necessary to ensure that individuals and businesses alike may protect not only their personal privacy, but their economic interests as well. H.R. 3378 is designed to extend protection to new categories of communications, and the Subcommittee is to be commended for addressing this vital question.

---

[1] Hearings on S.1667 Before The Subcommittee On Patents, Copyrights And Trademarks, Senate Judiciary Committee, November 13, 1985; see Opening Statement of Senator Charles McC. Mathias, Jr.; Opening Statement of Senator Patrick Leahy; Statement of the Honorable Robert W. Kastenmeier; Statement of the Honorable Carlos J. Moorhead.

Tandy supports the extension of privacy protection via H.R. 3378 to cellular communications as well as to all forms of encrypted communications. Given the technology of the cellular industry, including the hand-off of calls from cell to cell, the cellular telephone subscriber simply does not differentiate between cellular calls and conventional landline telephone calls. The subscriber thus perceives that, like wire communications, cellular calls are private and protected from interception. Similarly, encrypted transmissions are, by the very act of encryption, converted to a form of private communication and should be accorded privacy protection.

Accordingly, extension of Omnibus Act coverage to cellular and encrypted communications will conform existing statutes to the public's perceptions and expectations.

Tandy's sole, and limited, concern with H.R. 3378, as drafted, is that the bill may be overly-inclusive and extend privacy protection to categories of communications in which there has never been any perception or expectation of privacy. For example, as proposed H.R. 3378 would permit only the interception of ship-to-shore communications transmitted "for the use of the general public," and the interception of police or fire communications "readily accessible to the public," standards which are otherwise undefined.

As an alternative, Tandy proposes that H.R. 3378 be revised to proscribe the willful interception of encrypted transmissions or of communications transmitted between cellular radio telephones or between a cellular telephone and a landline telephone. This more narrow framing of the legislation would enable Congress to extend privacy protection to evolving communications technologies without unduly impairing the public's right to use its existing investment in radio receiving equipment.

## II. The Proposed Legislation

H.R. 3378 proposes to extend privacy protection to all electronic communications with certain specified exemptions.

These exemptions are, essentially, four in number: (1) communications designed to be "readily accessible to the public"; (2) communications transmitted for the use of the general public relating to ships, aircraft, vehicles or persons in distress; (3) communications transmitted by a walkie-talkie or a police or fire communications system designed to be readily accessible to the public; (4) communications transmitted by an amateur radio station operator or by a CB radio operator. H.R. 3378, Section 101(b). While the bill thus permits the use of walkie-talkies, CBs and police or public safety band-scanners (provided that such scanners monitor solely bands "readily accessible to the public"), it extends protection to other categories of transmissions broadcast over the public airwaves, including cellular telephone and ship-to-shore communications not made for the use of the general public.

Tandy endorses the extension of Omnibus Act coverage to all cellular communications. Indeed, it is clear that the typical cellular subscriber perceives and expects privacy in his or her cellular conversations. The Congressional Office of Technology Assessment has thus concluded:

> The public generally expects that telephone conversations are private and that electronic surveillance of telephone calls is illegal, except in very narrowly circumscribed law-enforcement and national security investigations. . . . [T]he new telephone technology was not envisioned when current

> legal protections were enacted, and thus the statutory protection against telephone surveillance is weak, ambiguous, or non-existent.[2]

In short, the similarities between landline and cellular service both in appearance -- e.g., the physical configuration of the subscriber handsets -- and service -- e.g., low call blocking rates and high grades of service -- have engendered in cellular subscribers the belief that their communications are "private." Indeed, giving the technological underpinnings of a cellular system -- e.g., the hand-off of calls and frequencies from cell to cell within the system's service area -- such a perception and expectation of privacy is justified and warranted.

As a practical matter, Tandy believes that extension of privacy protection will help ensure the continued growth and vitality of the cellular industry. Should protection be denied subscribers, cellular service could become less attractive vis-a-vis landline service. As the cellular industry is now in its infancy, denial of privacy coverage could well significantly impair the competitive viability of cellular technology. Tandy thus submits that the extension of privacy coverage to cellular communications could well serve the dual goals of fostering competition among the communications services, and encouraging the utilization of state-of-the-art technology.

---

[2] Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington, D.C.: U.S. Congress, Office of Technology Assessment, OTA-CIT-239, October, 1985) at 29.

Tandy also endorses extension of privacy protection to all encrypted transmissions. These communications are transmitted in a "coded" format. Accordingly, through the act of encryption, the message sender has demonstrated an intention and expectation that these communications remain "private". But, to date, privacy coverage is not afforded these messages unless they are transmitted by wire. Tandy supports the extension of the Omnibus Act to encompass encrypted communications and to conform existing laws to the public's perception and expectation of the scope of privacy coverage.

## III. The Proposed Approach

Tandy endorses the extension of Omnibus Act coverage to all cellular communications, but believes the bill should be amended to make it clear that it remains permissible to use scanners to monitor walkie-talkie, CB, police or public safety or ship-to-shore communications -- in other words, those communications that are now and historically have been "readily accessible to the public."

Tandy is, therefore, concerned that H.R. 3378, as drafted, is overly-inclusive. While amateur radio, CB and, to a limited extent, police and public safety band communications are excluded from protection, H.R. 3378 extends privacy coverage, for example, to certain ship-to-shore communications. Unlike cellular communications, however, these messages traditionally have not been thought by the message senders to be subject to privacy protection. The United States Court of Appeals for the Ninth Circuit has acknowledged, for example, that "scores of mariners. . . listen to the ship-to-shore frequency."[31] Given this fact and given the many years over which the maritime public has become used to monitoring ship-to-shore frequencies for reasons of safety, extension of privacy protection to these communications is not warranted.

Tandy believes that the perhaps inadvertent impact of H.R. 3378 on communications services to which there is no perception or expectation of privacy would be great. While the exact numbers are not available at this time, Tandy estimates conservatively that there are over 350,000 amateur radio operators in the United States, each typically owning more than one receiver; that there are between 40 to 60 million CBs and walkie talkies operational within the country; and that there are over 50 million short-wave multiband receivers. In total, there are perhaps over 120 million receivers which potentially could be affected by H.R. 3378. Clearly, legislation with the potential for such enormous impact upon the populace, and its accumulated investment, warrants careful consideration.

---

[31] United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (emphasis added).

In order to assure that equipment owners are not prohibited from maximizing the utility of their investment, Tandy proposes that the Subcommittee consider a more narrow approach, specifically legislation extending Omnibus Act coverage to all encrypted transmissions and all communications transmitted between cellular radio telephones or between a cellular radio telephone and a landline telephone. In this manner, protection would be afforded to, and the further development encouraged of, the new technologies which have evolved since adoption of the Omnibus Act. At the same time, however, the legislation would be framed in the narrowest manner possible to satisfy this goal, and the inadvertent impact upon other, traditionally unprotected, communication services (and equipment owners) would be avoided.

0074j

Mr. **Kastenmeier**. Thank you very much, Mr. Kuhnreich, for that brief, but I think very informative statement.

Our last witness on the panel and our last witness today is Mr. Richard T. Colgan. Mr. Colgan.

Mr. **Colgan**. Mr. Chairman and members of the subcommittee, I am Richard T. Colgan, executive secretary of the Association of North American Radio Clubs. I appreciate the opportunity to appear before you today to discuss H.R. 3378.

The Association of North American Radio Clubs is an affiliation of 18 of the oldest and largest nonprofit radio-listening organizations in North America. Fourteen of our member clubs are located in the United States and have a combined membership of more than 10,000 radio listeners.

In addition to representing our U.S. members, we believe that our concerns about this bill are representative of those which would be expressed by the millions of Americans, many of whom are elderly, and many of whom are disabled, who own and enjoy shortwave radios and scanners. These people have no one else to speak for them.

The numbers we have suggest that there are over 1 million shortwave listeners in America and that there are many millions more who own scanners.

As listeners we understand the vulnerability of some types of radio communications to interception. We agree with the major thrust of the bill that the Government interception of electronic communications must be carefully controlled and monitored. As a matter of principle, we applaud H.R. 3378's intent to provide that protection and we support its goals.

However, as a practical matter, we have serious concerns about the vague and overly broad language used in parts of the bill. That language could make it unlawful for Americans to listen to most of the radio spectrum. While this side effect was undoubtedly unintended by the bill's framers, the result could be an almost complete reversal of U.S. public policy.

Most of our concern stems from the uncertain meaning of "readily accessible to the public." The reality of radio waves is that they are present in our homes, our cars, our businesses, in this hearing room and other places, whether or not we want them there. All we need is a suitable receiver and we can hear those signals. A radio signal that pervades a populated area is, as a matter of physical fact, readily accessible to the public. With suitable protection, however, the information content of the transmission can be made private.

The broad sweep of the term "electronic communication" affords the same privacy protection to intruding and interfering signals as it does to ones operating lawfully. An example of this is a land mobile station interfering with a UHF-TV station. In that particular case, one could not lawfully intercept that signal to determine who it was interfering with their television so that the signal could be removed.

Now, there are several exemptions to the prohibition on listening that are contained on page 3 of the bill. We would offer the following major points about those.

First of all, we feel that H.R. 3378 makes general listening to those frequencies on which you would expect to hear distress calls unlawful.

Second, as a practical matter, there is no difference between signals from a radio that is carried in the hand, that is, a walkie-talkie, and one that is not.

Third, police, fire, business, forestry, mobile telephone, and international shortwave are equally accessible to the public.

In terms of amateur radio, the bill seems to exempt amateur auto patches, which are nothing more than private telephone calls with a wire-wireless interface.

We wonder why H.R. 3378 does not similarly exempt listening to other forms of mobile telephone calls.

Then, finally, pertaining to CB radio, the bill makes no specific mention of the general mobile radio service, or GMRS, which operates in the vicinity of 460 megahertz. That radio service is the original citizens band service and we assume that GMRS is not exempted from the prohibition on listening.

H.R. 3378 seeks to transfer the responsibility for communications privacy from the system provider or user to the general public. Since most land mobile services do not take even minimal precautions against interception of their transmissions, we believe they do not regard the privacy matter as a serious one.

We feel that if Congress wishes to extend privacy protection to land mobile or other radio services which have not generally had the expectation of such privacy, they should use the presence or absence of encryption as a test of whether the system provider or user expects that privacy.

The use of clear voice rather than encrypted voice is the difference between sending a postcard and sending a sealed letter.

Mr. Chairman, we had fully intended today to demonstrate to the committee how readily accessible such things as cellular telephones are. However, because of the questions that are presented by section 705 of the Communications Act of 1934, which, as you know, relates to the interception and the divulging, or the disseminating, of the information that is intercepted, we will not ask the committee to play that portion of our tape. We do have it available, however, for the committee's information.

With your permission, we would like to play two short tape segments which show how telephone conversations, or radio conversations in general, may be protected from true interception which has to do with the information content of those signals.

Mr. **Kastenmeier**. We would be pleased to hear you demonstrate this.

[Audio presentation.]

Mr. **Colgan**. Mr. Chairman, we could continue with that recording for some time. As I think you will admit, neither of those provided any of us in this room, unless there are people with powers far beyond those that I have, with the ability to understand the information that was transmitted.

We must ask why the bill shifts responsibility for system privacy away from the provider or user. The answer cannot be the lack of available technology as we just demonstrated. Radio communications privacy devices are in daily use by law enforcement agencies, the military, satellite operators, and private business.

The answer cannot be the cost of privacy systems. While the cost of some encryption devices may be high, consumer demand for privacy—and we have heard about consumer demand already this morning—and competition in the marketplace would be expected to drive prices down and increase the sophistication of encryption devices.

I might mention, Mr. Chairman, although it may be difficult for you to see these—and I don't dare remove them from the static protecting foam—this is an example of a microchip which could produce the signals that were the first that we heard, simple voice inversion.

[Microchip shown.]

Mr. COLGAN. That chip, by the way, costs, I think, $6.85, if you buy just one of them.

These are three examples of a very sophisticated type of encryption device which is now 2 years old. These can be purchased in the open market for around $40 for an individual piece. So the cost of the devices themselves is certainly not a factor.

[Microchips shown.]

Mr. COLGAN. It is interesting to note several things. First of all—and I don't know how long a string of numbers this would provide us with—Motorola provides digital voice protection for some of their radio equipment. I believe that in an attachment to my statement there is an example of some of that equipment.

Their digital voice protection equipment provides 2.36 times 10 to the 21st—and that is a tremendously long row of zeroes—of user programmable codes, that is, there are that many possible ways that that information can be encrypted. It is our understanding from a very quick calculation that using computers that are presently available, were you able to determine that a signal was indeed voice, and attempt to utilize these devices, it could take you as long as 4 years to hit upon the right code so that you could turn that signal into intelligible information.

I would like to offer a quote from the FCC if I might. We have borrowed this from the statement provided by the Satellite Television Industry Association, Inc., commonly known as SPACE. This is a statement from the Federal Communications Commission.

It says:

> It has long been the Commission's view that the initial responsibility for signal protection should be on the signal originator who is in the best position to protect the signal against an authorized interception in use.

Finally, Mr. Chairman, we believe that the bill would be virtually unenforceable. Radio receivers, unless they are used in public places, are generally undetectable in use.

The Association has offered four amendments which would go a long way toward alleviating our concerns.

First, we have provided a definition of the term "readily accessible to the public." We feel that the bill should be amended to include that any electronic communication which, first, is transmitted in an unscrambled or unencrypted manner and; second, shares a common type of modulation with other signals and; third, has a wide coverage area so as to be receivable in populated areas is considered to be readily accessible to the public.

Second, we regard listening to land, maritime, and air mobile communications, and shortwave fixed stations, as lawful under H.R. 3378.

If our interpretation is not what the bill intends, it should be amended so that it would not be unlawful to intercept an electronic communication made through an electronic communications system designed so that such electronic communication is unscrambled or unencrypted.

The third amendment. We are not aware of any Federal law or regulation limiting the purchase or ownership of any type of receiver. However, some of the rhetoric that has surrounded H.R. 3378 leads us to believe that efforts to impose such limits may be forthcoming. We would be much assured of the intent of all concerned if the bill were amended to state that it would not be unlawful to manufacture, sell, purchase, possess, or use any type of radio communications receiver for noncriminal purposes.

We feel this would simply make explicit what we believe to be present and traditional policy of the U.S. Government.

Finally, as amendment four, as worded, the bill provides the same measure of privacy protection to signals causing harmful interference as to lawfully present signals. To remedy this inequity, the bill should be amended to state that it would not be unlawful to intercept any electronic communication causing harmful interference to any lawfully operating station.

In summary, Mr. Chairman, while we support the intent of H.R. 3378, we are concerned that the unintended effects would make criminals of millions of Americans for listening to airplanes, trains and shortwave utility stations.

The Association of North American Radio Clubs stands ready to work with the subcommittee staff in developing a bill which truly represents the best interests of all Americans.

Mr. Chairman, this completes my prepared remarks. I would be pleased to answer any questions at this time.

[The statement of Mr. Colgan follows:]

**ASSOCIATION OF NORTH AMERICAN RADIO CLUBS**

STATEMENT

OF

RICHARD T. COLGAN
EXECUTIVE SECRETARY
ASSOCIATION OF NORTH AMERICAN RADIO CLUBS

BEFORE

THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

H.R. 3378, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985

ON

JANUARY 30, 1986

Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to appear before you today to discuss H.R. 3378, the Electronic Communications Privacy Act of 1985.

I would be surprised if any of you had heard of the Association of North American Radio Clubs prior to receiving copies of my testimony. Although we are a national organization founded in 1964, our work seldom brings us into the headlines. We are an affiliation of eighteen of the oldest and largest radio listening organizations in North America. Fourteen of our member clubs are located in the United States; four are headquartered in Canada. The combined membership in our U.S. clubs exceeds 10,000 radio listeners. These hobbyists listen to the radio frequencies from longwave to satellites; and from ordinary AM and FM signals to packet radio, radioteletype and facsimile broadcasts. Additional information on the Association is included in Attachment I.

In addition to representing our U.S. member organizations, we believe that our concerns about H.R. 3378 are representative of those which would be expressed by the millions of Americans who own and enjoy shortwave radios and scanners. While we cannot say with any certainty exactly how many Americans own these kinds of radios, there are some estimates available which convey the magnitude of those numbers.

Dr. Kim Elliott, Director of Audience Research at the Voice of America, cites a recent British Broadcasting Corporation (BBC) estimate that it has 2,000,000 regular listeners in North America. Because we can safely say that most shortwave listeners are BBC regulars, we can take this as a conservative guide to the total number of North American listeners. Even after subtracting listeners in Mexico and Canada, the number we are left with is about four times as many shortwave listeners in the U.S. as there are licensed radio amateurs (hams).

Estimates for the number of scanner owners are similarly difficult to find. The Electra Company (manufacturer of Bearcat scanners before the Bearcat line was purchased by Uniden in 1984) claimed that there were 8,000,000 scanners in homes, cars and offices around the country.

The Americans who own shortwave radios and scanners come from every walk of life; many of them are elderly and many are disabled. Radio listening is one way for them to find out what is happening in their communities, their country and the world. The vast majority of these casual listeners are unaware of H.R. 3378 and how it might affect them. Furthermore, the ambiguous wording of the bill has caused many hobbyists to believe that the provisions of the bill would not apply to them. These Americans are thus unable to have their voices heard. This is one of the reasons I am here today.

We see that H.R. 3378 has been shaped by the need to resolve various legal loopholes and contradictions created by changes in technology. It is visibly concerned with the status of electronic mail, computer data bases and with telephone-like wireless communications links. It addresses important questions of policy and fact.

The members of ANARC clubs understand, perhaps better than most, the vulnerability of some types of radio communications to interception and, thus, the importance of privacy protection. We agree with the major thrust of the bill that the intrusion of government into private lives, through the interception of electronic communications, must be carefully controlled and monitored.

The people we have talked with have not been worried about their cordless phone or mobile telephone conversations being overheard by casual listeners. To a person, however, they have expressed concern about the possibility that law enforcement and other government agencies could routinely and indiscriminately monitor those conversations.

If there is any concern about casual listeners misusing what they might hear, there is adequate remedy in Section 705 of the Communications Act of 1934. Vigorous, well-publicized enforcement of the Act by the Justice Department would be an effective means of assuring communications systems users that their conversations will be safe from disclosure by members of the general public.

Section 705 does not provide adequate protection from the improper actions of government. As a matter of principle, we applaud H.R. 3378's intent to provide that protection and we support its goals. However, as a practical matter, we have serious concerns about the vague and overly-broad language used in parts of the bill. That language could make it unlawful for Americans, whether hobbyists or casual listeners, to listen to most of the radio spectrum. While this is undoubtedly a side effect unintended by the bill's framers, the result could be an almost complete reversal of United States public policy relating to radio communications.

Portions of H.R. 3378 are so ambiguous that we do not know how concerned we should be about them. In other cases, the wording seems to make unlawful certain activities which contribute to public safety and the orderly use of the radio spectrum. In still other instances, the wording introduces radically new concepts about who bears the responsibility for protecting privacy of communications: concepts to which we must object and which we believe, upon thoughtful examination, will be seen as unnecessary.

## DEFINITION OF "READILY ACCESSIBLE TO THE PUBLIC"

Most of our concern stems from the uncertain meaning of "readily accessible to the public". The reality of radio waves is that they are present in our homes, cars, businesses, in this hearing room and other places, whether or not we want them there. All we need is a suitable receiver (and sometimes an antenna) and we can listen to those signals. A radio signal that pervades a populated area is, as a matter of physical fact, readily accessible to the public.

This statement is not as technologically simplistic as it may sound. Most radio system providers and users WANT their signals to be widely and easily heard. What they may NOT want is just anyone to have access to the INFORMATION carried by those signals. For that reason, we believe that the bill must clearly differentiate between the radio signal itself and the information it carries.

Most land-mobile services (including cellular telephones) use frequency modulation--FM--for their broadcasts. Although the channels are narrower than those used for the FM broadcasting with which we are all familiar, any FM broadcast receiver can be easily modified to tune in maritime and land-mobile channels. The same is true of AM radios and aeronautical stations.

Indeed, television sets can tune in some channels used for land-mobile communications because the FCC allocates unoccupied UHF TV channels for the use of land-mobile services. Because land-mobile stations normally use a common modulation type--FM--and broadcast their signals over wide areas, we can, again, only regard those transmissions as readily accessible. As we understand H.R. 3378, the use of the word "intercept", rather than "listen" or "monitor" is crucial and correct. "Intercept" refers to the acquisition of INFORMATION CONTENT; "monitor" or "listen" refers to the more general act of detecting the presence of a radio signal, irrespective of whether its content is intercepted. These definitions recognize the distinction between information which is private property and the radio spectrum which is a PUBLIC resource.

## DEFINITION OF "ELECTRONIC COMMUNICATION"

We also have difficulty with the sweeping, catch-all term "electronic communication". This term seems to originate with the idea that various forms of data are now fully interconvertible and the fact that the fixed telephone network, which formerly carried only voice, now carries a variety of non-voice communications. Furthermore, the phone system user cannot tell if his call is traveling by wire, optical fiber, microwave link or by satellite. Thus, combining all modes and channels under a single, general "umbrella" term--"electronic communication"--seems, at first glance, to make a great deal of sense.

While this might be convenient for those using the expanded telephone system, it does considerable violence to many well-established principles and practices in the field of radio communications: principles and practices grounded in the very real physical and legal differences between communicating by wire and communicating by radio.

Consider a voice message traveling by wire. The wire is physical private property, owned by someone. The information travels within an insulating, isolating sheath. To monitor that message, it is necessary to physically tap into that wire. The same message on radio travels on a public medium: it is neither insulated nor isolated. To listen to that message, there is no necessity for any physical connection between the receiving device (a radio) and the transmitting device. Considered separately, it would not be difficult to take into account the differences inherent in the two systems. It is only when these two are intermixed and interconnected that problems arise.

H.R. 3378 covers not only those communications systems which intermix and interconnect wire and wireless, but also wireless systems without such interfacing. The bill would seem to entitle some wireless systems to privacy protection equal to that of a wire system, irrespective of whether or not users of the service previously had some expectation of privacy or whether the type of communications allowed to such systems required that protection. Short of dispensing with the catch-all term "electronic communication", we cannot suggest a way to preserve the real and essential distinctions that exist between wire and wireless communication, both as to the regulation of their use and their physical features.

The broad sweep of the term "electronic communication" inadvertently creates some peculiar situations we know the Congress would wish to correct. For example, because of the channel sharing between UHF television stations and land-mobile services, it is all too common for a television viewer to be subjected to unwanted and harmful interference from a nearby land-mobile station. Should the TV viewer hear the content of the interfering signal, to avoid violating H.R. 3378, he or she should probably turn off the TV set. He or she certainly should not do what most knowledgeable people do--try to identify the interfering station so that action can be taken to cure the interference.

The bill would also prohibit individuals from monitoring their environments to determine if radio signals capable of causing physiological harm were present. Whether the presence of those signals constitutes trespass is a legal question. However, scientists are just beginning to study and understand the biological effects of exposure to various levels of electromagnetic radiation. To deny an individual the right to monitor radiation entering his or her home or body is to strip him or her of defense against what is becoming commonly known as "electropollution".

H.R. 3378 thus affords the same privacy protection to intruding, interfering and possibly harmful signals as it does to ones operating lawfully. We believe this is wrong and would make it much more difficult to identify and remove these unwanted signals.

"EXEMPTIONS" TO THE PROHIBITION ON LISTENING

If the bill were amended as we will suggest, that would resolve our concerns about the inconsistency and illogic of the "exemptions" to the prohibition on listening listed as sub-clause (ii) on page three of the bill. For the record, however, we would offer the following points:

DISTRESS CALLS. Unless a receiver is specially-equipped so that it can be turned on only by distress calls, one could not legally receive those calls. Without such a receiver, a listener would have to monitor every transmission on the radio frequency on which distress calls might occur. H.R. 3378 would seem to make such general listening unlawful.

WALKIE TALKIES. As a practical matter, there is no difference between signals from a radio that is carried in the hand and one that is not.

POLICE AND FIRE COMMUNICATIONS. Both the wording of the bill and testimony by the bill's sponsors indicate that they believe that police and fire communications are "readily accessible", but that other radio services--often just a few kilohertz or megahertz away--are not. In truth, there is no difference in accessibility between police, fire, business, forestry, mobile telephone, international shortwave, longwave beacons, and so on. A general-coverage shortwave receiver or a synthesized scanner can detect all of them with equal facility.

AMATEUR RADIO. The bill permits anyone to listen to ham signals. While we heartily endorse this provision, it does give us reason for wonder. The bill would seem to exempt amateur "phone patches" and "auto patches", which are nothing more than private telephone calls with a wireless-wire interface. As such, "auto patches" are little different from cellular or other mobile telephone calls. It is not apparent whether the bill actually exempts these "auto patches". If indeed it does, why does it not similarly exempt listening to all forms of mobile telephone signals?

CB RADIO. The bill permits anyone to listen to Citizens Band signals, presumably at twenty-seven megahertz. However, no mention is made of the General Mobile Radio Service (GMRS) at 460 megahertz, which is the original "citizens band" service. We must assume that GMRS is not exempted from the listening prohibition. Therefore, H.R. 3378 presumably prohibits the thousands of licensees in this service from listening to each other as is almost inevitable in the shared-frequency environment which exists. By prohibiting the monitoring of land-mobile channels, even by licensees, the bill makes compliance with the Federal Communications Commission's channel-sharing rules almost impossible.

## RESPONSIBILITY FOR COMMUNICATIONS PRIVACY

H.R. 3378 seeks to transfer the responsibility for radio communications privacy from the system provider or user (however they might wish to divide that responsibility) to the casual listener and the general public. We find it necessary to again stress the difference between the radio signal itself and the information (voice, data, video) carried on that signal. Merely receiving the signal in no way compromises the privacy of the information transmitted or that of the communication system user.

If the information is broadcast "in the clear", that is, it is not scrambled or encrypted, it is not difficult, in our view, to advance the arguments that: 1) the information content of the broadcast is not private, 2) the system provider does not intend that the information will be private, and 3) the system user has no reasonable expectation that the information will be private. Since most land-mobile services do not take even minimal precautions against interception of their transmissions, we believe that they do not regard this as a serious problem. The use of clear voice demonstrates to us a lack of concern for privacy of the communications. It is the difference between sending a postcard and sending a sealed letter.

We think that if Congress wishes to extend privacy protection to land-mobile or other radio services which have not generally had the expectation of such privacy, they may wish to use the presence or absence of encryption as a test of whether the system provider and the user expect privacy and to reinforce the technical protection in the bill's legal penalties.

As radio listeners, we recognize the realities of radio waves. As telephone users, we appreciate the feeling of privacy that the average American has whenever he or she uses the telephone. Manufacturers of communications systems have, or should have, similar perspectives. With this reasonable expectation in mind, we must ask why the bill seeks to shift responsibility for system privacy away from the provider or user?

The answer cannot be the lack of available technology. It exists today, and radio communications privacy devices are in daily use by law enforcement agencies, the military, satellite operators and private business. The answer cannot be the cost of privacy systems. While it is true that the cost of some encryption devices may be high, consumer demand for privacy and competition in the marketplace would be expected to drive prices down, just as we have seen happen for other forms of electronics technology. Additionally, we would predict that the sophistication of encryption devices would increase, providing even higher levels of privacy. Information on several encryption technologies and devices is included in Attachment 2.

Leaving the matter to the consumer is considered consistent with the trend--now nearly a decade old--of allowing market forces, rather than legislative decree, to determine the features of communications services offered to the public.

## ENFORCEMENT OF THE BILL

Finally, and we will not duell on this point, we believe the bill would be virtually unenforceable. Radio receivers, unless they are used in a public place, are generally undetectable in use. The authors of the Communications Act of 1934 realized this fact and did not make it unlawful to listen to any kind of wireless communications. The Act only makes it unlawful to "intercept and divulge" or disseminate the contents of those transmissions or use them for private gain. It is the Association's position that these provisions are as relevant and applicable today as when they were originally written.

## AFFIRMATIVE RECOMMENDATIONS

If the bill were amended to recognize the matters we have illuminated in a manner consistent with the facts, we would have no problem with it. In that light, the Association offers four amendments which would alleviate our concerns.

AMENDMENT ONE. There is no definition of "readily accessible to the public" in the bill nor have we seen or heard a definition which reflects the factual situation.

We believe we can provide such a definition. The bill should be amended to include the following: "Any electronic communication which 1) is transmitted in an unscrambled or unencrypted manner, and 2) shares a common type of modulation with other signals, and 3) has a wide coverage area so as to be receivable in populated places is considered to be readily accessible to the public."

AMENDMENT TWO. We believe it is unnecessary to make it illegal to listen to unscrambled or unencrypted transmissions, as the use of open voice demonstates a lack of concern for privacy. Because of the broad geographical coverage of some point-to-point wireless transmissions, combined with the use of open voice and common modulation, these stations are already "readily accessible." We regard listening to land, maritime and aeromobile communications and shortwave "fixed" stations as lawful under H.R. 3378. If our interpretation is not what the bill says or implies, it should be reworded as follows:

> "Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:
>
> > "(c) It shall not be unlawful under this chapter for any person--
> >
> > > "(i) to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is unscrambled or unencrypted."

By this amendment, we are asking only for the SAME rights for other radio listeners as those which have been accorded the owners of earth satellite receiving stations.

AMENDMENT THREE. We are not aware of any Federal law or regulation limiting the purchase or ownership of any kind of receiver, and we would oppose any change in this policy. Some of the rhetoric surrounding H.R. 3378 leads us to believe that efforts to impose such limits may be forthcoming. The recent California law prohibiting the manufacture, sale or purchase of any receiver solely capable of tuning the cellular telephone frequencies is an unfortunate example which we fervently hope never to see elevated to the Federal level.

We would be much assured of the intent of all concerned with this bill if the following amendment were inserted between lines 16 and 17 on page three, adding a sub-clause (iv) to Section 2511(2) of title 18, United States Code:

> "(iv) to manufacture, sell, purchase, possess or use any type of radio communications receiver for non-criminal purposes."

This would simply make explicit what we believe to be the present and traditional policy of the United States government.

Should the Congress wish to forbid or limit ownership of receivers capable of tuning specific portions of the radio spectrum, there are a number of inherent problems. Two of these problems are discussed in Attachment 3.

AMENDMENT FOUR. As worded, the bill provides the same measure of privacy protection to signals causing harmful interference as to lawfully present signals. To remedy this inequity, the bill should be amended by inserting sub-clause (v) after the sub-clause (iv) proposed above to Section 2511(2) of title 18, United States Code:

> "(v) to intercept any electronic communication causing harmful interference to any lawfully operating station."

## SUMMARY

The Association of North American Radio Clubs has thoroughly reviewed H.R. 3378 and its potential effects on the members of our affiliated organizations as well as on the millions of Americans who own and enjoy shortwave radios and scanners. While we support the intent of the bill, we believe the unintended effects would be disastrous. We are concerned that the bill would make criminals of Americans for listening to airplanes, trains and shortwave utility stations.

We have clearly stated our concern with the lack of definition of "readily accessible to the public" and "electronic communication". We have demonstrated the inconsistency and illogic of the "exemptions" to the prohibition on listening contained in the bill. We have correctly questioned the shifting of responsibility for communications privacy from the system provider or user to the general public. And we have pointed out the bill's unenforceability.

We have recommended four amendments to the bill which, in our judgement, clarify the bill's intent and correct its deficiencies. The usefulness of amendments two and four is dependent on whether there is agreement on the definition advanced in amendment one. Amendment three is desirable regardless.

The Association stands ready to work with the Subcommittee's staff in developing a bill which truly represents the best interests of all Americans.

Mr. Chairman, this completes my prepared remarks. I would be pleased to answer any questions at this time.

# ASSOCIATION OF NORTH AMERICAN RADIO CLUBS

## WHAT IS THE ASSOCIATION OF NORTH AMERICAN RADIO CLUBS?

The Association of North American Radio Clubs (ANARC) is a voluntary affiliation of eighteen of the oldest and largest non-profit hobby radio listening organizations in North America. ANARC was founded in 1964 to: 1) promote closer ties among radio clubs, 2) promote the interchange of information and ideas among member clubs, 3) work for the common good of the hobby, and 4) provide a medium to speak out for radio clubs and listeners in North America. In furthering these purposes, the Association maintains close ties with its counterparts in Europe--the European DX Council--and in the Pacific basin--the South Pacific Association of Radio Clubs.

ANARC is governed by a seven-person Executive Council, composed of an Executive Secretary and six members elected from among the executives of the member clubs; the Executive Secretary has no affiliation with any member club. Council members, as well as ANARC committee members and staff, serve as unpaid volunteers.

Fourteen ANARC member clubs are based in the United States; four are headquartered in Canada. These clubs have wide-ranging interests from longwave beacons (located below the standard "AM broadcast band") to long distance TV and FM reception to satellite signals. The combined

**Attachment 1**

membership of the fourteen American clubs exceeds 10,000 radio listeners.

Although the Association is composed of hobby clubs, it has, almost from its inception, been involved in national and international broadcasting matters. In 1966, it established a Frequency Recommendation Committee to work with such international broadcasters as Radio Sweden International, Radio Austria International and the Belgian Radio to find and maintain frequencies for the best reception of their shortwave signals in North America. Today, the committee regularly assists over a dozen international broadcasters.

Also in 1966, ANARC held its first convention in Kansas City, Missouri. Recent conventions have been held in Washington, DC (1983); Toronto, Ontario (1984); and Milwaukee, Wisconsin (1985). The twenty-second annual convention will be in Montreal, Quebec, July 18-20, 1986, hosted by Radio Canada International. These conventions, which are truly the "event of the year" for North American radio listeners, draw together hundreds of hobbyists, international broadcast personalities, manufacturers, dealers and listeners from around the world.

In 1983, ANARC was asked to assist the U.S. Department of State with preparations for the World Administrative Radio Conference on High Frequency Broadcasting. The Conference, held in Geneva, Switzerland early in 1984, discussed new strategies and technology for international broadcasting on the frequencies between six and twenty-six megahertz. Specifically, ANARC documented the effects of intentional harmful interference--jamming--on shortwave broadcasts intended for audiences in North America. The Association also furnished monitoring information on

1-2

the Soviet over-the-horizon radar systems (commonly called the "Woodpeckers" because of the sound of their signals) which regularly interfere with a wide range of stations on the high frequencies.

During 1985, ANARC's Over-the-Horizon Radar Committee organized and conducted the "Woodpecker Project" to gather current data on worldwide interference caused to shortwave broadcast stations by the high-power pulse emissions known as the "Woodpeckers". One hundred seven listeners in thirty-two countries participated in the Project. Information from the study is being analyzed and will be presented to telecommunications ministries of countries participating in the 1987 World Administrative Radio Conference on High Frequency Broadcasting to convince them to support a protocol statement condemning this interference.

The Association publishes a monthly twelve-page newsletter; produces regular programs for Radio Canada International and HCJB in Quito, Ecuador; and operates a computer bulletin-board for radio listeners.

ANARC may be contacted at Post Office Box 180403, Austin, Texas 78718-0403.

**STANDARD MICROSYSTEMS CORPORATION**

# COM9046

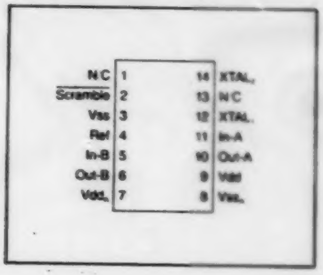
PRELIMINARY

# Single Side Band Speech Scrambler

## FEATURES

- ☐ Speech Scrambling/Descrambling
- ☐ High Dynamic Range
- ☐ Low Voltage Operation
- ☐ Low Power Consumption
- ☐ On Board Crystal Oscillator
- ☐ Uses Common Color Burst Crystal
- ☐ Full Duplex Operation
- ☐ Selectable Scramble Enable/Disable
- ☐ Switched Capacitor Filter
- ☐ COPLAMOS® n-Channel Silicon Gate Technology

## PIN CONFIGURATION



## GENERAL DESCRIPTION

The COM9046 is a monolithic integrated circuit containing a voice scrambler, a descrambler and a crystal oscillator. It is designed to provide speech communication equipment with a privacy feature. The COM9046 is also designed to operate with power supply voltages as low as ±2Volts. The low voltage operation and low power consumption of the COM9046 make it ideal for use in portable equipment.

Two identical speech channels are contained in the COM9046 for full duplex operation. Either channel is capable of performing the scrambling or descrambling function. These functions can be enabled or disabled via an external pin. The on-board oscillator employs an inexpensive 3.58 MHz TV color-burst crystal. Switched capacitor techniques are used to perform analog signal processing in the COM9046.

Typical applications for the COM9046 are Voice Communications, Cellular Phones, Wireless Phones, PBX's, Dictation Machines, Two-way Radios and Audio Recording Equipment.

Attachment 2

BEST COPY AVAILABLE

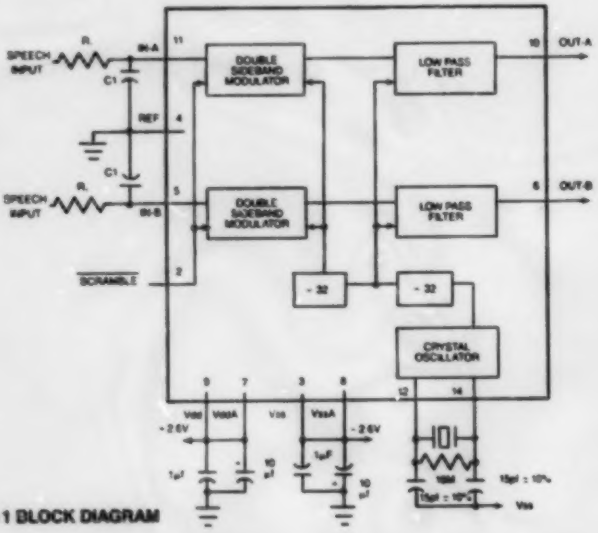


Figure 1 BLOCK DIAGRAM

## DESCRIPTION OF PIN FUNCTIONS

| PIN # | NAME | SYMBOL | DESCRIPTION |
|---|---|---|---|
| 1 | N/C | | No Connection |
| 2 | Scramble | — | Vss applied to this pin asserts the scramble; Vdd asserts non-scramble. |
| 3 | Digital Supply | Vss | Negative digital supply. Vss is typically − 2.6 volts with respect to pin 4. |
| 4 | Ref Input | Ref | Analog ground or mid-supply voltage. This is the chip 0 volt reference. |
| 5 | Audio Input B | In-B | Channel B audio input. D.C. voltage must be 0V with respect to pin 4. |
| 6 | Audio Output B | Out-B | Channel B audio output. DC voltage is 0V typical with respect to pin 4. |
| 7 | Analog Supply | $Vdd_A$ | Positive analog supply. Vdd is typically + 2.6 volts with respect to pin 4. |
| 8 | Analog Supply | $Vss_A$ | Negative analog supply. $Vss_A$ is typically − 2.6 volts with respect to pin 4. |
| 9 | Digital Supply | Vdd | Positive digital supply. Vss is typically + 2.6 volts with respect to pin 4. |
| 10 | Audio Output A | Out-A | Channel A audio output. DC voltage is 0V typical with respect to pin 4. |
| 11 | Audio Input A | In-A | Channel B audio input. D.C. voltage must be 0V with respect to pin 4. |
| 12 | Crystal input/ Ext Clock | $XTAL_1$ | Crystal Oscillator input or external clock. External clock frequency should be 3.58MHz with an amplitude of 4Vp-p and 0VDC. |
| 13 | N/C | — | No connection |
| 14 | Crystal input | $XTAL_2$ | Crystal Oscillator output. This pin is left floating when external clock is applied to pin 12. |

## OPERATION

Figure 1 shows a block diagram of the chip. Also shown in Figure 1 are the required external components.

Since switched-capacitor filters are used on the chip, the input speech signal must first be filtered by an anti-aliasing one-pole low pass filter before it is applied to the Audio input pin. The filter 3dB break point, which is determined by the product of C1 and R1 plus the output impedence of the audio source, should be less than 20KHz. This filter is required only if high frequency noise is present at the input. To maintain an output signal to noise ratio of 40dB, any unwanted signal higher than 3.5KHz contained in the speech input must be filtered to 40dB below the nominal speech input level, due to the fact that the on-chip modulator is switched at 3.5KHz.

The on-chip double sideband modulator can be turned on or off by asserting the SCRAMBLE input pin. The 3.5KHz switching frequency of the modulator is generated by dividing the output of the oscillator by 1024. The modulator output contains two sidebands centered at the suppressed switching frequency of 3.5KHz. The upper sideband is attenuated by a 4th order Butterworth lowpass filter. The filter, consisting of two biquad switched capacitor filters in cascade, is clocked at 111.9KHz. The inverted input speech spectrum appears at the filter output, and is available at the Audio Output pin. The filter output circuit is designed to drive a maximum capacitive load of 5pf in parallel with a minimum resistance of 15K ohms.

A parallel resonant crystal oscillator is employed in the device. The parallel resonant crystal should have a maximum series resistance of 150 ohms with a shunt capacitance of 5pf. To insure reliable oscillator performance, the components shown connected to XTAL pins 14 and 12 in Figure 1 should be used.

---

## ELECTRICAL CHARACTERISTICS

**COM9046**

**MAXIMUM GUARANTEED RATINGS*:**

| | |
|---|---|
| Operating Temperature Range | − 15°C to + 55°C |
| Storage Temperature Range | − 55°C to + 125°C |
| Lead Temperature (soldering, 10 sec.) | + 325°C |
| Positive Voltage on any pin with respect to Vss | + 6.5 V |
| Negative Voltage on any pin with respect to Vss | − 0.3 V |

*Stresses above those listed may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other condition above those indicated in the operational sections of this specifications is not implied.

NOTE: When powering this device from laboratory or system power supplies, it is important that the Absolute Maximum Ratings not be exceeded or device failure can result. Some power supplies exhibit voltage spikes or "glitches" on their outputs when the AC power is switched on and off. In addition, voltage transients on the AC power line may appear on the DC output. If this possibility exists, it is suggested that a clamp circuit be used.

**ELECTRICAL CHARACTERISTICS** (Ta = − 10°C to + 50°C, Vdd = Vdd$_A$ = + 2.6V ± 5%, Vss = Vss$_A$ = − 2.6V ± 5%.)

| Parameter | Min | Typ | Max | Units | Comments |
|---|---|---|---|---|---|
| Supply Current | | 5 | 8 | ma | |
| Insertion Loss | | 0 | 1 | db | |
| Audio Voltage Swing | | 0.8 | 1 | Vp-p | |
| S/N Ratio | 40 | | | db | |
| Modulation Frequency | | 3.5 | | KHz | |
| Bandedge of Sideband Filter | | 3.2 | | KHz | |
| Scramble Input High | Vdd-1.0 | | Vdd | V | |
| Scramble Logic Low | Vss | | Vss + .3 | V | |
| Input Resistance | | 5 | | M Ohm | |
| Dynamic Output Resistance | | 900 | | Ohm | |
| 3.5KHz Feedthrough | | − 80 | − 50 | db | |

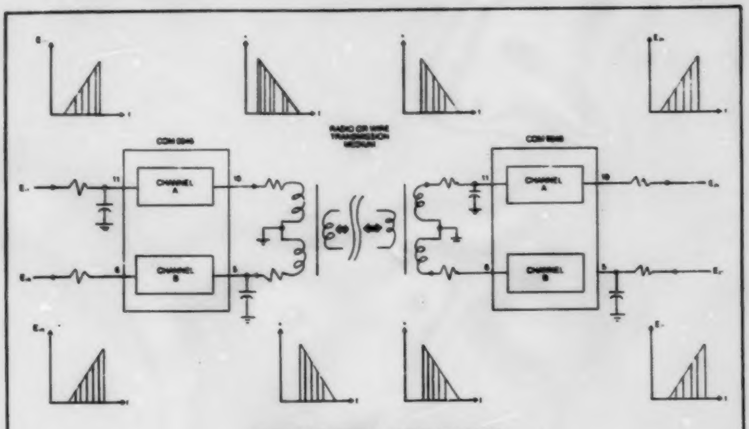


**Figure 2 TYPICAL APPLICATION**

*Inverted Frequency Spectrum of the Inspect Signals are Transmitted on the Transmission Medium

STANDARD MICROSYSTEMS CORPORATION

©1985 STANDARD MICROSYSTEMS CORP.

Circuit diagrams utilizing SMC products are included as a means of illustrating typical semiconductor applications, consequently complete information sufficient for construction purposes is not necessarily given. The information has been carefully checked and is believed to be entirely reliable. However, no responsibility is assumed for inaccuracies. Furthermore, such information does not convey to the purchaser of the semiconductor devices described any license under the patent rights of SMC or others. SMC reserves the right to make changes at any time in order to improve design and supply the best product possible.

STANDARD MICROSYSTEMS
CORPORATION

**TO:** All Field Sales

**FROM:** Jacques Hakim

**SUBJECT:** COM9046 Data Sheet

**DATE:** November 8, 1985

---

I am pleased to announce the availability of the COM9046 Data Sheet.

The release of the COM9046 voice Scrambler/Descrambler comes at a time when the need for privacy in voice communication systems is exacerbating. At the present time, there does not exist on the market a comparable product in the same price range, and that is the reason why the COM9046 is creating so much interest.

For your convenience, I have listed below the small quantity pricing for the COM9046 in plastic.

| | 1 - 24 | 25 - 99 | 100 - 999 |
|---|---|---|---|
| COM9046P | $6.85 | $5.70 | $4.75 |

Please contact your regional managers for production volume pricing.

In addition, please look for a series of Technical Sales bulletins on the device that will be released over the next few weeks.

**MOTOROLA**

# DVP Digital Voice Protection System

## MX 300 Series
## 2-way FM Portable Radio

136-174 MHz
403-430 MHz
440-512 MHz

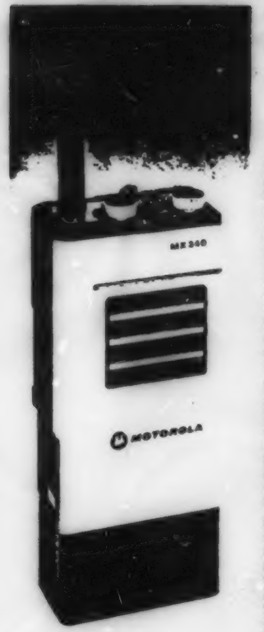
**Motorola's DVP Digital Voice Protection System** provides the user with the highest level of voice security commercially available today. To an unauthorized listener, a DVP radio transmission is totally unintelligible. Yet when this signal is properly decoded by a DVP receiver, clear audio comes through, providing the user with high intelligibility and excellent voice recognition.

To achieve the Digital Voice Protection System's high level security, a two step technique is utilized. First, regular speech is converted to digital speech using Continuously Variable Slope Delta Modulation (CVSD). This output is then scrambled through a highly sophisticated multi-register non-linear combiner algorithm. The resultant transmission contains no voice components and sounds like constant level random white noise.

Through the use of this digital scrambling technique, a huge number of unique and statistically unrelated codes are made available to the user—$2.36 \times 10^{21}$ (2,360,000,000,000,000,000,000). Any one of these codes can be electronically loaded into the secure memory of a DVP radio using the external Code Inserter. The code information contained in the memory of each radio and the Code Inserter cannot be recalled for display and these units will not reveal the code which is in use in a system. Thus, the DVP radio system makes it possible to restrict code information to a limited number of authorized individuals.

The MX300 series Digital Voice Protection Handie-Talkie radio belongs to the most advanced portable FM radio family available today. Its modular construction and extensive use of custom hybrid circuitry reflects the latest achievements in microelectronic technology. These techniques assure the ultimate in reliability, ease of maintenance and systems flexibility.

# DVP Digital Voice Protection Systems



## Security Features

- Digital Voice Scrambler
- Multi-register Non-Linear Combiner Code Algorithm
- $2.36 \times 10^{21}$ Orthogonal (unique) Codes
- All Codes Are User Programmable
- Random Code Key Initialization
- Self Synchronizing
- Internal Secure Electronic Code Storage
- Automatic Code Destruction With Power Loss
- Continuously Variable Slope Delta (CVSD) Modulation Analog To Digital Conversion

## Security Features • Benefits

**Multi-Register Non-Linear Combiner Code Algorithm** provides $2.36 \times 10^{21}$ user programmable codes. ● The coding algorithm and an incredibly large number of unique codes provide a very high level of security against unauthorized listeners, including more technically sophisticated eavesdroppers. All of the codes are unique and statistically unrelated. Only one code out of $2.36 \times 10^{21}$ possibilities will produce an intelligible output. There are no families of codes which are capable of providing a partially decoded output for similar codes.

**Random Code Key Initialization** occurs every time the transmitter is keyed. ● This random initialization provides increased security since the system will not reset its coding algorithm to the same place at the beginning of each transmission, but will initiate its coding process at a new starting point instead.

**Self Synchronizing** decoding eliminates delays at the beginning of transmissions or delays in system recovery after multipath or weak signal fades. ● Since no preamble is required, there are no delays or loss of information at the beginning of a transmission. In addition, a coded message will not be lost because no synchronization signal is received.

**Internal Secure Electronic Code Storage** within the radio unit eliminates code switches and does not reveal any knowledge of the code key by external visual or electronic probing. ● Consequently, code information is restricted to a limited number of authorized personnel.

**Code Insertion** into DVP radios is an operation which can be performed quickly and easily. ● The user can insert a new code into a DVP radio in a matter of seconds by connecting a DVP Code Inserter to the radio and pressing the code insert button. There are no mechanical keys required or switches which have to be set manually.

**Continuously Variable Slope Delta Modulation**, operating at a 12 Kilobit/second voice sample rate, is used to convert normal speech to digitized speech prior to scrambling and then back to normal speech after the receiver signal has been decoded. ● This A/D conversion technique, in combination with a new radio design incorporating optimized circuitry for digital voice transmission, coding and audio response, assures excellent voice recognition and high intelligibility.

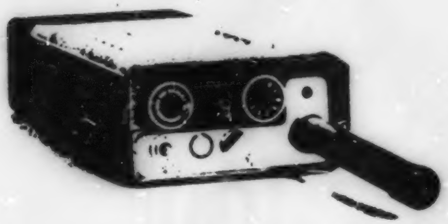
**Automatic Code Destruction With Power Loss** provides added code security. ● If someone attempts to tamper with a DVP radio and removes the code module, the code which it contains will be destroyed. To allow the user to change portable batteries, a time delay has been incorporated into the design of this feature to preserve code during this operation.

## Systems Features

- Complete system design capability
- Clear or coded operation
- Clear voice override (Private-Line Squelch models)
- Automatic or manual transmitter mode selection
- Private-Line Squelch compatible in clear mode
- Squelch tail elimination in the clear mode (Private-Line Squelch models)
- Clear mode alert tone prior to clear transmission
- Utilizes narrow band RF channels

## Systems Features • Benefits

**Complete Systems Design Capability**—The DVP MX series Handie-Talkie radio has been designed as part of a complete system of security radio which includes mobiles, base/repeater stations, microwave, and Total Area Coverage systems. ● A user can now, for the first time design a complete system



with voice security which includes a truly portable unit.

**Clear or Coded Operation** allows the user to transmit and receive either clear or coded messages. ● With this 2 mode operation, DVP radios can be used within existing clear radio networks as the user builds a security sub system. As the need arises or as old radios are replaced, the protected portion of the network can be expanded. Or a new all coded (or coded/clear) system can be designed to meet a user's specific communications needs.

**Clear Voice Override** automatically switches the receiver from the coded mode into the clear mode if an incoming message is clear voice (Private-Line models only). ● When operating in the coded mode the user will always get a message regardless of the mode in which that message was transmitted. Messages will not be lost and coordination problems among field units will be reduced.

**Automatic or Manual Transmitter Mode Selection** allows the user to manually select his transmission mode with the coded/clear switch or tie the mode selection directly to the channel selector, thus creating dedicated channels (coded only, clear only, or coded and clear). ● A user may thus be prevented from accidentally transmitting a clear message on a coded only channel. Similarly a user may designate a clear only channel in the radio for use on an existing system.

**Private-Line Squelch Compatibility** (Clear mode only) allows channel sharing among units on the same channel. ● In the clear mode, DVP radio units may access standard Private-Line Squelch equipped stations.

**Squelch Tail Elimination** is provided through the use of a reverse burst in the clear mode (Private-Line Squelch units only). ● Operators will not be disturbed by any annoying squelch tail or noise burst at the end of a transmission.

**Clear Mode Alert Tone** is emitted prior to a clear transmission. This tone warns the sender that he is about to transmit non-protected information. ● Thus, he will not mistakenly transmit private information in the wrong mode.

**Narrow Band RF Channel Bandwidths** permit the use of 25 KHz or 30 KHz channel spacing. ● DVP radio systems do not require extra wide channels or special channel assignments.

## Radio Features Options

The DVP Handie-Talkie Radio incorporates the DVP security features with the features and options of the versatile MX300 series portable radios. For a complete list of features and a more detailed discussion of each feature, please refer to the individual MX300 radio series catalog sheets.

### Radio Features

- Single integrated unit containing radio and scrambler circuitry.
- Unique phase lock loop transmitter.
- Sensitron single conversion receiver.
- Multiple RF power levels. (1w, 2.5w, 5w in VHF; 1w, 2w, 5w in UHF)
- 8 (6 VHF) frequency capability.
- Transmit/battery status indicator.
- Twist off batteries with 4 available battery sizes.
- Weather sealed push to talk.
- Externally accessible fuse.
- External jacks for antenna and speaker.

### Radio Options

- Time out timer.
- Converta-Com compatibility for mobiles use.
- RF preamplifier (VHF only).
- Remote speaker microphone.
- Surveillance accessories.

# DVP MX-300 Series 2-Way FM Portable Radio

## Performance Specifications

### Security

| | |
|---|---|
| Scrambler Type: | Digital |
| Coding Method: | Multi-Register Non-Linear Combiner |
| Number of Codes: | 2.36 x $10^{21}$ orthogonal (unique) codes |
| Synchronization: | Self synchronizing (no preamble required) |
| Code Key Initialization: | Random |
| Code Key Generation: | External hand held microprocessor controlled code inserter (Cat. T3010__X) |
| Code Storage: | Volatile Electronic Memory |
| Number of Codes Per Radio: | One |
| Analog to Digital Conversion: | Continuously Variable Slope Delta Modulation (CVSD) |
| Voice Sample Rate: | 12 Kilo Bits/Sec |

### Size

2.84" wide x 1.41" deep x (see chart below) high (72 mm x 36 mm x    mm)

| | MX340 | MX350 | MX360 |
|---|---|---|---|
| Radio Only: | 4.96" (126 mm) | 5.76" (146 mm) | 6.36" (161 mm) |
| Radio with battery: | 1 Hour Rapid Charge Batteries | | |
| Light Capacity: | 6.45" (164 mm) | 7.23" (184 mm) | 7.82" (199 mm) |
| Medium Capacity: | 6.81" (173 mm) | 7.59" (193 mm) | 8.18" (208 mm) |
| High Capacity: | 8.53" (216 mm) | 9.31" (237 mm) | 9.90" (252 mm) |

**Weight:** Radio only (average)

| | | |
|---|---|---|
| T2-R2 carrier squelch | VHF | 16.4 oz (465g) |
| | UHF | 16.3 oz. (462g) |

**Additional weight for features/options:**

| | |
|---|---|
| Private-Line Squelch | +.2 oz. (6g) |
| Each additional channel VHF | +.4 oz. (11g) |
| Each additional channel UHF | +.2 oz. (6g) |

**Batteries Only**

1 hour radio charge

| | |
|---|---|
| Light capacity: | + 5.2 oz. (147g) |
| Medium capacity: | + 7.3 oz. (207g) |
| High capacity: | +14.1 oz. (399g) |

**FCC Designations:***

UHF

| | | 450-512 MHz |
|---|---|---|
| 1 watt | 2 Frequency | [illegible] |
| 1 watt | 4 Frequency | [illegible] |
| 1 watt | 6 Frequency | [illegible] |
| 1 watt | 8 Frequency | [illegible] |
| 2 watt | 2 Frequency | CC4231A |
| 2 watt | 4 Frequency | CC4232A |
| 2 watt | 6 Frequency | CC4233A |
| 2 watt | 8 Frequency | [illegible] |
| 5 watt | 2 Frequency | CC4234A |
| 5 watt | 4 Frequency | [illegible] |
| 5 watt | 6 Frequency | [illegible] |
| 5 watt | 8 Frequency | [illegible] |

All Receivers RC5862

VHF

| | | 136.0-174 MHz |
|---|---|---|
| 1 watt | 2 Frequency | CC3256A |
| 1 watt | 4 Frequency | CC3257A |
| 1 watt | 6 Frequency | CC3258A |
| 2.5 watt | 2 Frequency | [illegible] |
| 2.5 watt | 4 Frequency | CC3261A |
| 2.5 watt | 6 Frequency | [illegible] |
| 6 watt | 2 Frequency | [illegible] |
| 6 watt | 4 Frequency | [illegible] |

All Receivers RC5861

---

* Licenseable under FCC Rules & Regulations Part 90 for Police and Fire Services.

For International usage, local PTT regulations apply

### Radio

| | VHF | UHF |
|---|---|---|
| Model Series: | H23, H33, H43AXU | H24, H34, H44AXU |
| Frequency: | 136-174 MHz | 403-430, 440-512 MHz |
| Channel Spacing: | 30 KHz | 25 KHz |
| Power Supply: | One rechargeable nickel-cadmium battery | |

### Transmitter

| | VHF | UHF |
|---|---|---|
| RF Power Output: | 1W/2.5W/6.0W | 1W/2.0W/5.0W |
| Frequency Stability: (−30°C to +60°C, +25°C Ref): | ±.0005% | ±.0005% |
| Modulation—Clear<br>Coded: | 16F3, 15F2, 16F9<br>20F3Y | 16F3, 15F2, 16F9<br>20F3Y |
| FM Noise: | −50 dB | −50 dB |
| Audio Response¹: | +1, −3 dB from 6 dB/octave pre-emphasis from 300 Hz to 3 KHz | +1, −3 dB from 6 dB/octave pre-emphasis from 300 Hz to 3 KHz |
| Audio Distortion¹: (At 1000 Hz, 3 KHz deviation): | 3% | 3% |
| Spurious & Harmonics | | |
| 1 Watt: | −67 dB | −67 dB |
| 2.5 Watt (2.0W UHF): | −71 dB | −58 dB |
| 60 Watt (5.0W UHF): | −75 dB | −53 dB |
| Frequency Separation: (No degradation) | 12 MHz | 6 MHz |

### Receiver

| | VHF | | UHF |
|---|---|---|---|
| Modulation Acceptance: | | ±7.5 KHz | ±7.5 KHz |
| Sensitivity: | W/O PREAMP | WITH PREAMP | |
| 20 dB Quieting¹: | .5 µV | 20 µV | .5 µV |
| 12 dB SINAD¹: | .35 µV | 20 µV | .35 µV |
| Selectivity (EIA SINAD): | 80 dB | 80 dB | 80 dB |
| Frequency Separation (No degradation): | 2 MHz | 4 MHz² | 1 MHz |
| Intermodulation: | 80 dB | 75 dB | 75 dB |
| Frequency Stability (−30°C to +60°C; +25°C Ref): | ±.0005% | ±.0005% | ±.0005% |
| Spurious & Image Rejection: | 80 dB | 80 dB | 60 dB |
| Audio Output¹: (@ less than 5% distortion): | 500 mV | 500 mV | 500 mV |

---

[1] Specification applies to clear mode only. Performance in the coded mode has been tailored to deliver optimum intelligibility and voice recognition.

[2] Separation of 10 MHz possible with sensitivity degrading to .35 µV (20 dB Quieting), or 12 MHz separation possible with sensitivity degrading to .5 µV.

**Support Services**

Wherever Motorola sells, our product is backed by service. In the U.S., we have 900 authorized or company-owned centers. In addition, our products are serviced throughout the world by a wide network of company or authorized independent distributor service organizations.

MOTOROLA
Communications and Electronics Inc.

A subsidiary of Motorola, Inc.
1301 E. Algonquin Road, Schaumburg, Illinois 60196
Telephone (312) 397-1000

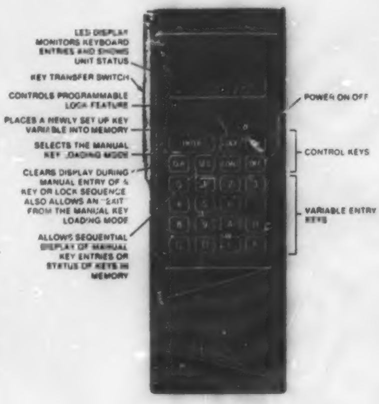
Specifications subject to change without notice.

Ⓜ, Motorola, Sensitron, Private-Line, DVP, Handie-Talkie and MX300 are trademarks of Motorola Inc. © 1981 by Motorola Inc. Printed in U.S.A. (8112) Mont

## DES Option

| Features | Description | Benefits |
|---|---|---|
| **Federal Government Approved Digital Encryption Algorithm** | The National Bureau of Standards has established DES as the common standard for protecting all forms of digital communications used by Federal agencies Motorola's DES Voice Encryption System conforms to NBS specifications | Motorola's DES radio system has been approved for use when sensitive informations must be transmitted |
| **Plug-In Modules** | DES Encryption modules are fully compatible with their DVP encode/decode module counterparts in all Digital Voice Protection equipment | Existing DVP radios can be retro-fitted with DES Encryption modules quickly and economically The need to purchase new radios or devise special electronic interfaces is eliminated |
| **Secure Communications** | A DES-equipped DVP radio can operate on any one of 70 quadrillion (70.000.000 000.000.000) key variables Each key variable creates a unique and orthogonal encryption with no possible "cross-talk" or partial decoding between any two different keys | Radio system security is enhanced by the large number of available key variables Using the DES key variable loader keys may be quickly and easily changed at any time |
| **Automatic "Self-Tests"** | The radio's DES module tests its encryption output every time a transmission is initiated. allowing only properly encrypted messages on the air. | Self testing increases the radio system security provided by DES Self testing does not delay communications |
| **Key Variable Transfer Verification** | The radio's DES module tests the key variable input to verify that the entry is valid The module also automatically exercises its encryption, decryption and self testing functions immediately after a key is loaded The module must pass all tests before it will transmit a DES encrypted message | This automatic key verification and testing sequence allows the user to perform both types of tests with only one, simple action Transfer verification further enhances system security and reliability |
| **Factory or Field Installable** | DES may be purchased as either an option to a new DVP radio, or as a factory tested field replacement module for existing DVP radios | To convert existing DVP systems to DES operation, simply exchange the DVP modules for DES modules No other modifications on standard equipment are required |

**DES Key Variable Loader shown with DVP Portable**


LED DISPLAY MONITORS KEYBOARD ENTRIES AND SHOWS UNIT STATUS
KEY TRANSFER SWITCH
CONTROLS PROGRAMMABLE LOCK FEATURE
PLACES A NEWLY SET UP KEY VARIABLE INTO MEMORY
SELECTS THE MANUAL KEY LOADING MODE
CLEARS DISPLAY DURING MANUAL ENTRY OF A KEY OR LOCK SEQUENCE ALSO ALLOWS AN "EXIT" FROM THE MANUAL KEY LOADING MODE
ALLOWS SEQUENTIAL DISPLAY OF MANUAL KEY ENTRIES OR STATUS OF KEYS IN MEMORY
POWER ON OFF
CONTROL KEYS
VARIABLE ENTRY KEYS

# DES Option

**Performance Specifications**

| | |
|---|---|
| **DES option number:** | W 388 (mobile radios)<br>H 388 (portable radios)<br>C 388 (base stations) |
| **Scrambler Type:** | Digital |
| **Coding Method:** | Data Encryption Standard (DES)<br>—Complies with the applications requirements of Federal Information Processing Standards (FIPS) 46 and 81, and the Commercial Voice Radio Requirements of Federal Standard 1027 |
| **Number of Keys:** | 7.2 × $10^{16}$ unique, orthogonal key variables |
| **Synchronization:** | Self synchronizing (no preamble required) |
| **Initialization:** | Internally derived pseudo-random initializing vector |
| **Key Variable Generation:** | External handheld key loader, Model No. T3020 X |
| **Number of Keys per Radio:** | One (DVP Dual Code Select option not available) |

**Shipments to countries outside the United States require a State Department munitions license for DVP products.**

**Support Services**
Wherever Motorola sells our product it is backed by service. In the U.S. we have 900 authorized or company owned centers. In addition, our products are serviced throughout the world by a wide network of company or authorized independent distributor service organizations.

MOTOROLA
Communications and Electronics Inc.

A subsidiary of Motorola, Inc.
1301 E. Algonquin Road, Schaumburg, Illinois 60196
Telephone (312) 397-1000

Specifications subject to change without notice.

®, Motorola and DVP are trademarks of Motorola Inc.
© Copyright 1981 by Motorola Inc. Printed in U.S.A.

(B111) 5M

R3-17-1-10

**SBS NEWS**

For Immediate Release
Tuesday, Sept. 17, 1985
No. 85-32

## SBS OFFERS TRAFFIC PROTECTED SERVICE OPTION TO SAFEGUARD COMMUNICATIONS

**McLEAN, Va., Sept. 17** -- A new Traffic Protected Service (TPS) that provides a communications option for businesses that require a higher level of security was announced today by SBS.

SBS's Traffic Protected Service enables U.S. Government contractors to meet a Department of Defense requirement to begin protecting unclassified transmissions related to national security. The service is also expected to appeal to financial institutions and other organizations who want to protect their transmissions.

SBS's TPS option is available to SBS Skyline$^{(sm)}$ WATS customers for implementation in January 1986.

With the implementation of the service option, SBS becomes the first common carrier to encrypt satellite transmissions for a public switched network offering. SBS encryption is transparent to customers and will be implemented without affecting service. Digital encryption units encode and decode transmissions at sending and receiving SBS Network earth stations. Where required, SBS will assist customers in the protection of service access circuits connecting customer premises to SBS Network earth stations.

-more-

TPS supplements the transmission security already inherent in SBS's all-digital system. A protection capability has been available to SBS's dedicated private network customers since mid-1984.

TPS uses the Data Encryption Standard (DES) specified by the U.S. National Bureau of Standards in an enhanced, SBS-proprietary implementation.

SBS applies multiple levels of safeguards to ensure communications protection of transmissions via satellite. At the first level is the inherent privacy of SBS transmissions from various earth stations in random bursts of variable durations. Next, traffic is encoded according to the DES algorithm. SBS further compounds the protection by frequently changing the master and working keys.

The option's low cost is achieved by integrating encryption capabilities into SBS's existing satellite-based TDMA (Time-Division Multiple-Access) system. Only one "black box" encryption unit is required at each SBS Network earth station. SBS Protected Service is available for a one-time charge of $85 per access port, plus a usage charge of 1.2 cents per call minute. Additional charges apply for protection of service access circuits, which may be required in certain areas of the country.

SBS, the communications company owned by IBM and Aetna, provides a family of Skyline services to more than 220,000 customers nationwide.

# # #

For further information:
Gunnar Hughes, SBS Public Affairs
703-442-5523
Home: 703-830-8208

ASSOCIATION OF NORTH AMERICAN RADIO CLUBS

## TWO PROBLEMS ASSOCIATED WITH LIMITING OR FORBIDDING OWNERSHIP OF RADIO RECEIVERS TUNING CERTAIN FREQUENCIES

Should the Congress wish to forbid or limit ownership of receivers capable of tuning through specific portions of the radio spectrum, we would point out that a simple device called a frequency converter, added to a legal receiver, would overcome any band limitation. Frequency converters can be inexpensively built using the most common electronic parts. Thus, we regard the receiver band-exclusion approach as unworkable and easily defeated. However, we must mention the special hardship such an approach would impose on shortwave listeners, because of the unique organization of the shortwave bands.

The shortwave part of the radio spectrum is defined as 3 to 30 megahertz. It is made up of over one hundred small sub-bands, some only a single channel wide. There are many types of stations using these frequencies: international broadcasters such as the Voice of America, the BBC and Radio Beijing; civil aircraft crossing oceans; merchant mariners; foreign news agencies; domestic broadcasters in the Tropics; and ionospheric research radars, to name only a few.

**Attachment 3**

All these stations need to operate in this band because shortwave signals propagate over very long distances. But they only propagate long distances in certain parts of the shortwave spectrum, and the active parts change over time in daily, seasonal and decade-long cycles. To ensure that the tens of thousands of stations that need long-range propagation can get it throughout the daily and seasonal cycles, the various services are tightly interleaved. Some services share bands, so that one can hear VOA and, at the same time on the same channel, hear a radioteletype station as well.

To complicate matters, some bands are very overcrowded; others are underfilled. This has led to an unauthorized redistribution of stations, where broadcasters have moved into Fixed Service bands, adding to the mixture of point-to-point and broadcasting stations.

Because of the tight interleaving of service allocations, virtually all shortwave receivers cover most all of the shortwave spectrum--not just the bands allocated to broadcasting, but ship-to-shore, air-to-ground, amateur radio and Fixed Service bands, too. If coverage were to be limited to just the bands allocated to broadcasting, not only would shortwave listeners not be able to tune in many broadcasts, they would still be able to tune in many non-broadcast stations sharing the broadcast bands.

Mr. **Kastenmeier**. Thank you very much, Mr. Colgan.

Your organization differs from that of Mr. Williams insofar as you represent essentially listeners and he represents people that operate radios—ham radio operators.

Mr. **Colgan**. I think there is a great deal of crossover, Mr. Kastenmeier. Many of the members of our organizations are licensed radio amateurs, and many of the licensed radio amateurs who are represented by Mr. Williams tune to the shortwave utilities or they own scanners. So, I think while the league's position and ANARC's position may differ, there is a commonality there which might not on its surface be apparent.

Mr. **Kastenmeier**. Interestingly enough, we just heard a few moments ago Congressman Swindall's radio page device which was communicating, of course, a confidential message, to him. The question is: Should he alone be able to receive that or should anyone who cares to tune in and be able to hit on his band receive Congressman Swindall's message? That is one of the questions I think is a policy question for the committee.

Let me ask, Mr. Kuhnreich, because I think you made a distinction which Mr. Williams and Mr. Colgan perhaps might have a different point of view about, and that is the cellular telephone. You indicated that probably other devices, there was not an expectation of privacy and that they would not necessarily have the protection. But that a cellular telephone, you felt, there was an expectation of privacy.

Mr. Colgan indicated that it is possible to have for such a technology, use it for—to encrypt it. And, indeed, was a demonstration, Mr. Colgan, that which would be used for a cellular telephone that you gave us in terms of the encryption?

Mr. **Colgan**. Either of the devices which were demonstrated could be used for cellular telephones. Obviously, the first one, which was simple voice inversion, is the bottom line, if you will, in terms of privacy protection.

The digital voice protection is many, many steps up that ladder. The chips that we were demonstrating here, which are the National Bureau of Standards standard for digital encryption, are as close as we can put our hands on to being the state of the art today.

Mr. **Kastenmeier**. Before I pursue the question with Mr. Kuhnreich, what are those particular devices currently most commonly used as encryption devices? With respect to what technology? In what context are they most commonly used today?

Mr. **Colgan**. I am not certain of that answer. I do know that the DES chips are used in protecting various types of data by corporations. It is the standard, again, that the National Bureau of Standards has adopted and has recommended to the Federal Government.

I believe that that technology is already being used by the Federal Government at this point in time. However, I will be happy to provide you with a precise answer to that question.

Mr. **Kastenmeier**. Fine.

Mr. Kuhnreich, in terms of retailing or selling cellular telephones, to what extent is it common, or is it available, to sell encryption devices with those cellular telephones?

Mr. **Kuhnreich**. I have not seen any, Mr. Chairman.

**Mr. Kastenmeier.** It is not common to do so?

**Mr. Kuhnreich.** No, sir.

**Mr. Kastenmeier.** It would have to be new implementation of that technology?

**Mr. Kuhnreich.** I might point out, Mr. Chairman, that the tape played by my learned and distinguished friend on my left was played on a Radio Shack Tandy Corp. tape deck, so it is meaningful to me to some degree.

However, if we were talking about an incremental cost of $5, I assure you, sir, I wouldn't be here today, if that is all we are talking about. My understanding is in order to have some foolproof protection on a cellular mobile radio, we are talking in terms of $3,000 or $4,000 a unit compared to $11.99.

**Mr. Kastenmeier.** As you indicated, at least indirectly, one would have a problem if you are using a cellular telephone gaining access to a person on a wired telephone system—which you can do, as I understand—using encryption with an ordinary device. If you gain access into an AT&T or other system, any encryption that you would use could be decoded, or could be applied to any other system.

**Mr. Kuhnreich.** Ninety-nine percent of calls on the cellular mobile radio networks today originate on a wire line phone. It is rare that one cellular telephone talks to another.

The first thing, Mr. Chairman, is you do not know most of the time that it is a cellular mobile telephone.

I will pay a compliment to Southwest Bell—back in Fort Worth we can't tell, the reception is so perfect. So, here is a fellow on the phone, he is talking someone on the cellular mobile phone—he has no idea that he is open to interception.

**Mr. Kastenmeier.** Of course, you represent Tandy, but do you have any notion of how many cellular phones are already owned by consumers in this country?

**Mr. Kuhnreich.** Yes, sir. Approximately 200,000.

**Mr. Kastenmeier.** How many scanners could intercept or have the capability of intercepting those 200,000?

**Mr. Kuhnreich.** Our best guess is that at this particular time there are somewhere between 4 and 5 million scanners out in the hands of the public, most of which could be modified to intercept cellular mobile. Very few have been sold with the express purpose of intercepting cellular mobile. Cellular mobile is only about 2 years old and it is not exected to get into high gear for another 18 months.

**Mr. Kastenmeier.** Most scanners could not because they would have to be modified?

**Mr. Kuhnreich.** That is correct, Mr. Chairman.

**Mr. Kastenmeier.** But as someone on the staff indicated, and I would like comments of either Mr. Williams or Mr. Colgan. Regency Electronics of Indianapolis advertises a scanner system suggesting you can also listen to weather, business, and marine radio calls, plus radio telephone conversations that offer more real life intrigue than most soap operas. And with our new models there's even more.

**Mr. Colgan.** Mr. Chairman, if I might.

**Mr. Kastenmeier.** Yes, Mr. Colgan.

Mr. **Colgan**. We find that line of advertising, although it may well be true that that excitement exists, we find that line of advertising inappropriate. I think it appeals to a very small segment of the potential market for scanners. Most people who buy scanners want to listen to the aircraft band, want to listen to planes come and go from National, for example. They want to listen to maritime; they want to listen to the Coast Guard; they want to listen to police, fire, EMS, for whatever reason.

I don't think there are that many people out of the 3 to 5 million—and we certainly wouldn't dispute that figure—a very small portion of those people who, on a regular basis, listen to those kinds of broadcasts.

Mr. **Kastenmeier**. Mr. Colgan, my own surmise is that the case is as you stated. However, we must attempt to look at the picture as a whole as to where we might be going, to what extent encryption is the answer, and to what extent other types of decisions might be made to discourage this type of overhearing. That is what the bill attempts to address.

I should yield, I think, to my colleague, Mr. Boucher.

Mr. **Boucher**. Mr. Chairman, I have no questions.

Mr. **Kastenmeier**. All right.

Mr. Williams, would you like to comment, too, on ham radio operators? Are ham radio operators traditionally the same as persons who use scanners? We know that there is, up to 2 million people that use scanners in the country.?

Mr. **Williams**. As Terry says, there is a great deal of overlap. A lot of our folks do have scanners. Our folks are apt to be interested in anything electronic. We are big in computers. We are using digital communications ourselves—pocket radio is the new game in town. It has grown from 4,000 people being capable last spring, to over 10,000 now, and it is just a curve that is going straight up.

Many of us own computers and we are doing digital things. Many of us own scanners. And we may have a semiprofessional interest in the scanners because we have been so tied up doing emergency work for people. So, we want to be aware of what is going on with the police and fire department and to assist when we can. If their circuits get overloaded, we pitch in, because we have got radios that are ready, being tested every day for our own purposes, and they are ready whenever the providers of safety services get overloaded. So, yes, a lot of us do have scanners.

Just in answer to your general question, nobody has brought out the fact that there are a great many television sets that tune up to channel 88. The top channels were the place where the Government got the territory for cellular. So, all of those older television receivers were intended to receive these frequencies that the cellular is now on.

So, in terms of potential, there are a lot of people who can listen. We think that education of the public that their conversations may not be totally private would be perfectly appropriate by the cellular industry.

Mr. **Kastenmeier**. We certainly recognize the communications policy needs of radio operators and listeners. As a matter of fact, you made reference to the fact that the legislation itself attempts to state that it is not unlawful to do a number of things, including intercepting electronic communications which is transmitted by a station for use of general public which relates to ships, aircraft, vehicles, persons in distress, or by a walkie talkie, or a police or fire communications system, et cetera, et cetera, or by an amateur radio station operation, by a citizen band radio operator, et cetera.

We may not have anticipated all the exclusions nor have drawn it up from a policy standpoint as precisely as we need to, or would wish. That is one reason we welcome testimony certainly of the three of you, and others. Paradoxically, and there has been some reference to it, we have a similar problem with respect to television, satellites and cable. We have very convoluted questions of what should be received and where it is appropriate for someone to either be compensated or to have these transmissions private. They often merge. These policy questions are so pervasive that we even have the policy question quite obviously in terms of national security and other particular interests, and how we can accommodate the various interests that Government and that individuals legitimately have. And it will be our job, in considerations of communications policy as well as of other considerations, to see whether we can draft a bill which appropriately accommodates the various interests.

That will be a challenge, and it will be an ongoing one. Obviously, the three of you represent slightly different interests, but still an array of interests, which I think have to be responded to.

I must honestly say, I think to some extent that the concerns either have been addressed or may not be necessary to address. Not to be argumentative, but I know that Mr. Colgan suggested that maybe we need to have a special section about the manufacture of all this equipment. We frankly did not think that would be necessary. We think that is implicit but we will certainly consider it. It was not our intention to make unlawful the manufacture of any such equipment.

Nonetheless, this is certainly an area in whch the Congress must act—I hope not precipitously, but reasonably expeditiously—because the new technology has rendered fire legislation in prior acts of the Congress, literally obsolete. We are getting more and more court cases because we have not filled in the gaps in terms of what the policy of the American people is as represented by legislation and by an updating of legislation.

I want to express my thanks to the three of you as witnesses in this endeavor this morning.

That concludes today's testimony.

We will have a fourth day of hearings on the subject which will be announced in the very near future.

The committee stands adjourned.

[Whereupon, at 11:35 a.m., the subcommittee was adjourned.]

BLANK PAGE

# ELECTRONIC COMMUNICATIONS PRIVACY ACT

---

WEDNESDAY, MARCH 5, 1986

House of Representatives,
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice,
Committee on the Judiciary,
*Washington, DC.*

The subcommittee met, pursuant to call, at 1:35 p.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier, Moorhead, and Coble.

Staff present: David W. Beier and Deborah Leavy, counsel; Joseph V. Wolfe, associate counsel; and Audrey K. Marcus, clerk.

Mr. **Kastenmeier**. The committee will come to order.

This afternoon the subcommittee is holding its fourth and final hearing on H.R. 3378, the Electronic Communications Privacy Act of 1986.

This subcommittee first held hearings in 1978 on the need to reform the wiretap law and to take other steps to protect the privacy of citizens. Pending before us then were bills by myself, Mr. Fish, and others, which were in part predicated on the views of the dissenters—myself included—from the Report of the Wiretap Commission. Some of those bills were eventually enacted into law as the Right to Financial Privacy and the Foreign Intelligence Surveillance Act. While those measures were important compromises between legitimate law enforcement concerns and privacy, we unfortunately left reform of the Federal wiretap law behind.

The bill before us today continues the tasks we began nearly a decade ago. What gives me a renewed sense of optimism is that this bill has attracted a wide range of support from the business community.

This bill is supported by AT&T, ADAPSO, the Electronic Mail Association, and other companies and trade associations.

This business support has really two sources. First, the industry is concerned about obtaining protection from improper private interceptions. Second, they are concerned about protecting their customers' privacy from unwarranted Government intrusions. This business consensus is a new and important change in the terms of the debate about privacy.

Perhaps the most heartening development in our work has been the bipartisan support the bill has generated. My colleagues Carlos Moorhead and Tom Kindness deserve special recognition, as do other cosponsors on the subcommittee: Rick Boucher, Bruce Morrison, Pat Schroeder, and Howard Berman. In total there are 35 cosponsors from both parties and across the political spectrum. This breadth of support gives me confidence that when we mark this bill up in the near future we can preserve consensus.

This afternoon the subcommittee will hear from two witnesses from a law enforcement perspective. The first witness is Mr. James Knapp of the Department of Justice. The second witness is Mr. Clifford Fishman, a former prosecutor and consultant to the President's Organized Crime Commission.

Before we commence, let me make one final comment. The bill before us today is more than a cellular bill or an electronic mail bill; it is an attempt to rationalize an important privacy law with new technologies. We should not lose sight of what is being protected. The means of communication is perhaps not so much that which we seek to protect as a sanctity of our expressions.

Perhaps through consideration of the bill we will be able to reach the goal enunciated by the Supreme Court that our communications "are as fully guarded from examination and inspection as if they were retained by the parties forwarding them."

Does my colleague have an opening statement?

Mr. **MOORHEAD**. I just wish to join you, Mr. Chairman, in welcoming the witnesses here this afternoon, and look forward to their testimony.

Mr. **KASTENMEIER**. We are delighted to greet Mr. James Knapp of the Department of Justice today. He is Deputy Assistant Attorney General representing the Criminal Division. Mr. Knapp, we have your statement, which is a long one, a 27-page statement. If you would like to introduce your colleague, and if you could abbreviate your statement we would receive the balance of it in full for the record.

## STATEMENT OF JAMES KNAPP, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, ACCOMPANIED BY FREDERICK D. HESS, DIRECTOR, OFFICE OF ENFORCEMENT OPERATIONS, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Mr. **KNAPP**. I certainly thank you. Mr. Chairman, Congressman Moorhead.

I appreciate the opportunity to appear here today to discuss H.R. 3378, the Electronic Communications Privacy Act of 1985.

Sitting with me on my left is Mr. Frederick Hess, Director of the Office of Enforcement Operations in the Criminal Division, who will assist me in answering any questions which you may have.

I have prepared an abbreviated version of my testimony which I will now read to you.

Since receiving this bill to amend title III of the Omnibus Crime Control Act of 1968, the Department of Justice representatives have had ongoing discussions with staff members of both this committee and the Senate Subcommittee on Patents, Copyrights and Trademarks. As you know, the committee has proposed identical legislation.

The discussions have involved trying to develop effective proposals for amending title III to cover new technology without jeopardizing legitimate law enforcement interests. In addition, the Department, in conjunction with several Federal law enforcement agencies, has conducted an in-depth review of the existing legislation to ascertain how the new developments in technology can best be addressed. In some areas it was decided that amendments to the existing legislation would be most effective, while in other areas new legislation appears to be the best way to proceed.

As you know, on November 13, I appeared before the Senate subcommittee to express our concerns about the proposed bill. You have that testimony and I would request that it be incorporated in the record. I do not propose to go over that again. At the time I had testified, the internal Department study had not been completed. It has now been completed.

In reviewing the proposed legislation, there was concern a complete overhaul of the structure of title III would impair the effectiveness of the statute. The parameters within which Federal agencies must function have been clearly defined by 18 years of case precedent. Redefinition of its provisions would require reinterpretation by the courts. This could result in confusion and uncertainty. The Department feels title III should be left as much intact as possible.

The Department recognizes that some of the new forms of technology should be brought under legislative control. Some of the new technology is so similar to traditional telephone conversations that it belongs within the framework of title III. Other types of technological development like electronic mail and computer transmissions using wire facilities which are primarily nonaural communications should be incorporated in a new statute. This way the new statute will stand on its own and will not effect existing case precedent under title III.

In my testimony today, I would like to address, first, those technological developments that should be incorporated in title III; and, second, those new technological developments for which new legislation should be sought. I will also discuss recommendations prepared by the Department to amend the general provisions of title III to make it more effective.

First of all, technological developments that should be incorporated into existing title III legislation.

The three primary areas of concern are: cordless or handheld telephones; tone and voice pagers; and cellular telephones.

Part of cordless telephone conversations are by wire and part are by radio transmission that is readily interceptible by a citizen with an ordinary radio receiver.

The leading Federal decision in this area, *United States* v. *Hall,* held that because a conversation was in part by wire, title III applies. At least three State courts have held that this produces an absurd result, and we agree. We think cordless telephones should be regulated by title III, but there should be no reasonable expectation of privacy as to the radio portion of those conversations unless they are encrypted in some manner.

This would also protect the citizen who inadvertently intercepts such a communication from criminal liability. The same logic applies to tone and voice pagers. All you need to intercept them now is a compatible device tuned to the same frequency. Like cordless telephones, logic dictates that the radio portion of the calls should only be accorded a reasonable expectation of privacy where it is encrypted in some manner.

Like cordless telephones, cellular telephones function primarily by wire and part by radio. While initially secure, at least when they were first manufactured, because of the frequencies utilized, many cellular telephone calls are now easily intercepted, although only on a random basis. These radio transmissions are more difficult to intercept than cordless telephones, however.

We also recognize that many people have and use cellular telephones and do have at least a subjective expectation of privacy in their use. For these reasons, the Department is prepared to support legislation that would require title III authorization for all law enforcement officers, for all portions of cellular telephone calls.

Further, we believe devices should be outlawed which are manufactured for the purpose of intercepting cellular communications, or conversations.

We also believe a citizen should be subjected to criminal and civil liability at least where a call is intercepted and divulged for a purpose that is illegal, tortious, or for commercial gain. Now, the cellular industry would like a broader statute that would cover intentional or malicious interception of a cellular phone call.

We have some concerns about the enforceability of such a statute, but we have agreed to meet with industry representatives to review this issue sometime in the immediate future. In any event, we do not believe there should be liability for unintended interception.

The second category: Technological developments for which new legislation should be drafted.

The new legislation should incorporate several types of nonaural communications like electronic mail and computer transmissions. Any proposed legislation should recognize the different characters of these types of transmissions. Depending on the level of intrusion, different mandates should be developed for each type of interception.

The communications that we believe should be covered can be divided into four stages: First, interception of prospective transmissions of the substance of a communication.

Second, interception or seizure of substantive data temporarily stored in a data bank of a communications common carrier prior to the final transmission of the data to the recipients electronic mail box and its actual receipt.

Third, seizure of substantive data temporarily or permanently stored in the files of the communications common carrier as a record of the transaction.

Fourth, transactional data other than substantive information maintained in the records of the common carrier indicating the date and time of the communication and its sender and receiver.

The Department feels generally that as to prospective transmissions, electronic mail should not be accorded more protection than first-class mail. First-class mail can now be seized by a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure. However, since the level of intrusion during the transmission is higher than when it is stored, the transmission, we feel, should enjoy some of the protections of title III. These would include all the protections afforded under rule 41, plus specificity of the facility, the type of information sought to be intercepted, minimization provision, and a directive that the order only be for a specified duration up to 30 days.

The bill should have provisions to protect the integrity of the tapes. The admissibility of evidence should be determined by existing case law. The judge should have the power under the bill to direct the cooperation of a carrier and the legislation should provide the carrier with civil immunity for that cooperation.

The bill should apply to direct communication between parties as well as to those where a third-party common carrier is involved, and should apply to the use of private facilities not necessarily involving the facilities of interstate commerce.

Unlike title III, however, approval from a designated official in Washington should not be required for its use. The Department would require some type of supervised reapproval in the field by regulations.

The order should be obtainable for any offense for which a search warrant can be issued. It should not be necessary to show that all other investigative procedures have failed. The order should be issued by a magistrate as well as a judge as is now the case for search warrants. Annual reports should not be required.

The second category: Interception of substantive data temporarily stored in a data bank prior to final transmission.

In these situations, the communication is analogous to a first class piece to mail. A search warrant under rule 41 should suffice, signed by a magistrate or judge. The order or warrant should be issuable for any offense under State or Federal law. Like a warrant, a 10-day period should be alloted for its execution. A prosecutor in the field should be empowered to make the request of the court for such a warrant.

Third category: Seizure of data temporarily or permanently stored in the files of a communications common carrier.

Substantive data that has become part of the record should be available by the service of a grand jury subpoena. Fourth amendment requirements are inapplicable to this type of situation. There is a well settled principle of law that documents given over to third parties do not enjoy privacy protection barring some privilege situation.

Final category: Seizure of transactional data maintained in the records of the common carrier.

This type of nonsubstantive administrative data like identification of the sender/receiver, the date or time of the transmission, and the subscriber, is not subject to privacy protection. The seizure of this information is not a search within the meaning of the fourth amendment. This information should be available by the service of a grand jury subpoena by or an administrative subpoena the Federal law enforcement agency where provided for by law.

Any new legislation like title III should have consent provisions where the prior approval of one of the participants has been received.

Video surveillance. This is an area where there are at present no statutory provisions and where we recommend a statute be enacted to cover situations wherever there is the invasion of a reasonable expectation of privacy.

Two basic types of situations: First, the interception of visual images being transmitted from point to point, that is, closed circuit television.

Second, the direct interception of images within a place where there is a reasonable expectation of privacy, like in a house or office.

The leading Federal case authority, *United States* v. *Torres*, establishes parameters for the use of television surveillance that the Department feels balances the privacy interests of the public with the needs of law enforcement.

This decision held that where there was sufficient specificity of the location, crime sought, a showing that normal investigative procedures had failed, a specified period of duration, and a minimization provision, the court could issue such an order.

A procedure based generally on the requirements of rule 41 and adding those title III requirements specified in *Torres* would, in our view, afford appropriate privacy protections.

We also would like to request an amendment to make it clear that you could get such an order as part of a title III order without the present procedure now getting two separate orders, where a title III is being separately sought.

For the same reasons discussed in connection with title III and the new legislation, this type of legislation should also, of course, contain consent provisions where the prior authorization of one of the parties has been received.

Expanded coverage of title III. I would like to recommend several specific proposals to make the current title III statute even more useful than the last 18 years have proven it to be.

The original drafters of title III sought to minimize its use to forestall abuses, although over 18 years experience has taught that abuses have been almost nonexistent. The time has come to reevaluate that thinking. Title III is so well understood today that there is no reason to limit its application to a limited list of offenses.

The Department recommends the statute be expanded to cover all felonies and at a minimum several offenses not currently covered by title III are clearly so serious that whatever happens they should be added to the list, and those are specified in the testimony. But just to name a few: threatening Federal officials; destruction of energy facilities; destruction of aircraft or aircraft facilities; hostage taking; murder for hire; and violent crimes in aid of racketeering.

Title III should include a provision to allow the Acting Assistant Attorney General in charge of the Criminal Division to authorize title III requests when the Assistant Attorney General is unavailable.

A provision should be included in title III allowing for the interdistrict use of an eavesdropping device in a vehicle, or bug, where the vehicle temporarily travels from district to district during the interception period.

Under present law, a new order is necessary in each district into which the vehicle travels no matter how long it is there.

A provision should be included in title II for an interception order to be issued targeting an individual at whatever facility within the jurisdiction of the court that he or she is using at a given time, as opposed to the authority to intercept only at a particular facility.

Another provision in title III that would be very helpful to law enforcement would be the authority to use support personnel under the close supervision of an investigative or law enforcement officer to assist in the execution of a title III.

Further, a provision should be included in title III to provide for after-the-fact minimization of foreign language conversations where particular foreign language experts are not reasonably available during the interception period. The judge should have the authority to authorize this under the particular circumstances of a case.

A provision should be included in title III providing for a good faith exception to the exclusionary rule as enunciated in *United States* v. *Leon* for ordinary search warrants.

One item has arisen that is not in my prepared testimony but which I would like to recommend at this time. In the Comprehensive Crime Control Act of 1984, a section was added to title 18 making it an offense to warn a person that his property was about to be the subject of a search warrant. It is 18 U.S.C. 2232. We believe a similar offense should be created making it a crime to warn a person that he or she is the target of an electronic surveillance court order.

In conclusion, I would like to reiterate that a great deal of thought has been given to the development of these recommendations. We feel that these amendments to title III and the new legislation for nonaural communications comprise reasonable standards that the Department of Justice and the Federal law enforcement agencies could support. Naturally, the details of each proposal require further specification. However, the principles are viable and should provide legislative guidance in those areas for years to come barring unforeseen developments. The Department is committed to working with your staff and with the Senate staff to produce effective legislation.

That concludes my formal remarks, Mr. Chairman. I would be happy to answer any questions which you have.

[The statement of Mr. Knapp follows:]

**U.S. Department of Justice**

*Washington, D.C. 20530*

STATEMENT

OF

JAMES KNAPP

DEPUTY ASSISTANT ATTORNEY GENERAL

CRIMINAL DIVISION

BEFORE

THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE

ADMINISTRATION OF JUSTICE

COMMITTEE ON THE JUDICIARY

UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

H.R. 3378, ELECTRONIC COMMUNICATIONS PRIVACY ACT

ON

MARCH 5, 1986

## TESTIMONY ON H.R. 3378

Mr. Chairman and members of the Subcommittee, I appreciate the opportunity to appear here today to discuss H.R. 3378, the Electronic Communications Privacy Act of 1985.

The bill, H.R. 3378, as well as S. 1667, an identical bill proposed by the Senate, is intended to amend the provisions of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. 2510 et seq., relating to electronic surveillance to cover the advances in technological developments in electronic communications, both aural and non-aural, that have occurred since the passage of the original legislation in 1968.

Since receiving the proposed legislation, Department of Justice representatives have had ongoing discussions with staff members of both this Subcommittee and the Senate Subcommittee on Patents, Copyrights and Trademarks to try to develop effective proposals to amend Title III to cover the new technology.

In addition, the Department, in conjunction with several law enforcement agencies, has conducted an in depth review of the existing statutes to ascertain how the new developments in technology can best be addressed in new legislation or in the amendment of existing legislation.

On November 13, 1985, I appeared before the Senate Subcommittee on Patents, Copyrights and Trademarks to express some of the Department's concerns based upon our review of the proposed legislation. Copies of that testimony have been provided to staff members of this Subcommittee, and I will not at this time specifically reiterate all of the objections set forth in my testimony today other than to reiterate that several provisions of the bill do create serious problems for law enforcement.

At the time I testified before the Senate Committee, the Department had not completed its internal review of the legislation and could offer only general views on various aspects of, and potential law enforcement problems associated with, the bills. As indicated, our review has now been completed. At this time, therefore, in an effort to move constructively and specifically address these matters I would like to suggest those subjects in which the Department could support new legislation relating to electronic communication.

In reviewing the proposed legislation, we came to the realization that a complete overhaul of the structure of Title III would impair the overall effectiveness of the existing statute. The parameters within which federal enforcement agencies and the Department were intended by Congress to function under Title III have been clearly defined through nearly two decades of case precedent. The statute works well and it is the Department's position that, while some improvements or refinements are appropriate, its basic scope should be left intact as much as possible. Complete redefinition of Title III's provisions would require new interpretation by the courts. This could result in an extended period of confusion and uncertainty in the law which would not benefit either law enforcement or the public at large.

A second concern that was identified during our review of the proposed legislation was the escalation of the level of judicial supervision with respect to other investigative methods used in conjunction with Title III investigations that do not rise to the level of intrusion addressed by Congress in the original legislation. Subjecting these lesser investigative methods (which in many instances do not even constitute a "search" within the meaning of the Fourth Amendment) to strict substantive and procedural requirements would only have a substantial adverse effect on law enforcement. Moreover, escalating the level of judicial supervision in these areas would not appreciably enhance the privacy of our citizens over the levels they now enjoy based upon existing Departmental regulations in these areas. I am referring primarily to (1) the securance of telephone toll and other business records; (2) the use of pen registers; (3) the interception of tone and non-aural paging devices; and (4) the use of location detection devices (beepers). It is our firm belief that present controls and case law in these areas provide adequate safeguards against abuse. Our legislative recommendations do address "tone and voice" pagers where there are Title III implications.

On the other hand, since the passage of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. 2510 et seq., we recognize that technology has rapidly evolved in the areas both of aural and non-aural transmissions of communications that is not addressed by current statutes. The Department shares with the proponents of H.R. 3378 the belief that it is desirable that some of these forms of technology be brought under legislative control with respect to interception of such communications by both law enforcement agencies and private individuals. In our view, there is new technology that is so similar to traditional telephonic communication that it belongs within the framework of Title III; to that extent Title III should be amended accordingly. With respect to the other types of technological development, such as electronic mail and computer transmissions using wire facilities, it is the Department's position that a new statute should be developed to address this enhanced technology.

In my testimony today, I would like to address, first, those technological developments that should be incorporated into Title

III; and, second, those technological developments for which new legislation should be drawn. I will also discuss recommendations prepared by the Department, based upon its review, for amending the general provisions of Title III to enable law enforcement authorities to better effectuate its mandates.

## I. TECHNOLOGICAL DEVELOPMENTS THAT SHOULD BE INCORPORATED INTO THE EXISTING TITLE III LEGISLATION.

The three primary areas of concern are: (a) cordless or handheld telephones; (b) cellular telephone technology; and (c) tone and voice pagers.

A. Cordless or Handheld Telephones. In this type of communication, part of the transmission is by wire and part is by radio. The radio part of the transmission can readily be picked up by anyone listening to commercially available radio equipment such as an AM radio receiver or a scanner. Under existing law, a private citizen intercepting such a communication could conceivably incur criminal liability. There is a serious question as to whether there should be a reasonable and justifiable expectation of privacy with respect to this type of transmission.

The leading and virtually only federal decision in this area is United States v. Hall, 488 F.2d 193 (9th Cir. 1973), in which a radio telephone in an automobile was used to communicate to a traditional telephone on land. This conversation, partly using wire facilities and partly using radio transmission, was held to be within the proscriptions of Title III because the present statute refers to transmissions "in whole or in part by wire." Title III under this premise would apply here regardless of the expectation of privacy because it was "in part" a wire communication. At least three state appellate courts have held that this produces an absurd result. The absurdity lies in the fact that statements overheard by an ordinary radio receiver become illegal interceptions and are deemed inadmissible in court. Although in the past we have felt bound in interpreting Title III to follow Hall because it is the only federal decision on the matter, we are inclined to agree that the result is inappropriate from a policy standpoint. See Dorsey v. State, 402 So. 2d 1178 (Fla. 1981); State v. Howard, 679 P.2d 197(Kan. 1984); State v. DeLaurier, 488 A.2d 688 (R.I. 1985)

A reasonable approach to this situation in our view would be to make Title III applicable to situations in which the wire portion of a cordless telephone conversation is to be intercepted, or to situations in which there is to be an interception of the radio portion of the transmission only where the radio portion has been encrypted and is therefore not readily accessible to citizens using ordinary radio equipment. There should be no expectation of privacy where the radio portion of the transmission can be intercepted in analog (regular voice) form. The interception of such a conversation should not impose either criminal or civil liability on either a citizen or law enforcement official. Indeed, most cordless phones carry a written warning that interception of conversations by third parties is possible. A law enforcement officer should not be subject to any greater liability than a citizen under these circumstances. In the event the conversation is encrypted, affirmative steps would have to be taken to intercept it and under these circumstances an expectation of privacy can be deemed to be reasonable.

B. Cellular Telephone Technology. Cellular telephone transmissions also involve communications that are transmitted in part by the use of wire facilities and in part by the use of radio transmissions. Such technology is most commonly used in car telephones and in portable phones contained in briefcases. Like cordless telephones, a citizen with a scanning device can readily intercept all or portions of the communication depending on conditions at the time. These calls are not as readily interceptible as cordless telephone conversations because of the likely mobility of at least one of the participants during the transmission and because of the varying technology. By their nature, cordless phones must remain in relatively close proximity to one base unit. The radio transmissions in cellular technology are assigned to geographical "cells" and the frequencies on which the transmissions are conducted change at random as the sender or receiver passes geographically from cell to cell. The interceptor would have to follow the vehicle to intercept the call as it passes from cell to cell and would have to scan within each cell to find the appropriate randomly assigned frequency in each cell. However, since the cellular conversation can be readily intercepted if these procedures are followed, the cellular transmission conceivably should be entitled to no more reasonable expectation of privacy than the cordless transmission unless it has been encrypted in some way.

We recognize, however, that a significant number of people have and use cellular telephones and at least subjectively have an expectation of privacy in their use in much the same way as they do with a conventional telephone. A similar subjective expectation of privacy does not exist with hand held telephones which, as noted, often carry specific warnings from the manufacturer. For that reason, even though we would prefer that the radio portion of these transmissions be encrypted to fully support the reasonable expectation of privacy, we are prepared to accept legislation that with respect to cellular technology would require Title III authorization for law enforcement officers to intercept either the wire or radio transmission portion of cellular communications. We also recognize that technology in the cellular telephone area is developing very rapidly and it will only be a matter of time until the communications common carriers develop equipment that will either encrypt the calls or secure the transmissions in some other manner.

We do think, however, that citizens scanning for recreation purposes should not incur criminal or civil liability. To forestall that result, we feel that the bill should contain a provision that a citizen will only incur criminal or civil liability where the citizen both intercepts and divulges the communication under circumstances in which the interception and divulgence are illegal, tortious, or for commercial gain. We feel that this would provide a proper balance between the needs of law enforcement and the rights of ordinary citizens.

However, to address the problem of citizen interception, we think that consideration should be given to outlawing devices manufactured in the future that are used to intercept cellular telephone conversations, at least where they are primarily designed for that purpose.

Another problem that must be addressed when considering amendments to Title III is providing coverage under the statute for the growing number of private telephone companies operated often by large commercial entities that may not use the facilities of a common carrier operating such facilities in interstate commerce. It ought to be made clear that these types of telephone companies are covered under the provisions of Title III.

C. Tone and Voice Pagers These types of paging devices transmit an aural message to the paging device in the possession of the subscriber by means of a transmission that is in part by use of wire facilities and partially by the use of radio transmission. Based upon existing technology, they are readily susceptible to interception by an individual with a compatible device on the same frequency. Much like the cordless telephone, placing it under Title III simply because some portion of the communication uses a wire produces an absurd result since it can so readily be intercepted during the radio portion of the communication. Again, a more realistic approach is to make Title III applicable to interception of the wire portions of the transmissions and to the radio portion only where the radio portion is encrypted. An interception under these latter circumstances would require affirmative steps to accomplish the interception and an expectation of privacy can therefore be deemed to be reasonable.

## II. TECHNOLOGICAL DEVELOPMENTS FOR WHICH NEW LEGISLATION SHOULD BE DRAFTED.

The principal other types of new technology that I will address relate to the non-aural transmission of communications through the use of wire facilities. The technology includes electronic mail and other types of transmissions accomplished by the use of computers connected to the facilities of communications common carriers or in some cases private transmission facilities. The term "communications common carrier" is a term utilized in H.R. 3378. Initially it should be redefined to include the companies now providing what is known as "electronic mail" and computer data providers and revisers.

Any proposed legislation must in our view recognize the different degrees of privacy related to this type of transmission at its various stages. Depending upon the level of intrusion involved, different mandates should be developed for the interception of this type of communication. The communication can be divided into four stages: first, interception of prospective transmissions of the substance of a communication; second, interception or seizure of substantive data temporarily stored in a data bank of the communications common carrier prior to the final transmission of the data to, and its receipt by, the recipient; third, seizure of substantive data temporarily or permanently stored in the files of the communications common carrier as a record of the transmission after its receipt; and, fourth, transactional data other than substantive information maintained in the records of the communications common carrier indicating the date and time of the communication and its sender and recipient.

A. Authority to Intercept Prospective Communications. This authority is authority to intercept electronic mail or other type of computer transmissions that will be sent in the future. It is analogous to Title III interceptions in which the court order directs the interception of telephone calls to be made in the next 30 days. The level of intrusion here is greater than situations in which the data is merely stored, yet is still somewhat less than in the case of ordinary telephone calls in which the communication is immediate and unchangeable. We believe the interception of electronic mail should include some but not all of the procedural requirements of Title III. The authorization to intercept the communication should be accomplished by a statute mandating a judicial authorization based upon probable cause akin to that which can now be secured with a Fourth Amendment search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure. This procedure is based on the premise that the interception of electronic mail generally should be accorded no more protection than that accorded to regular mail. At the present time regular mail can be seized with a Rule 41 search warrant. Electronic mail due to its use of telephone lines should, in our view, enjoy only certain of the additional protections provided by Title III due to its unique nature.

The search warrant or other judicial authorization should be based upon a sworn affidavit establishing probable cause to believe that a crime has been, is being, or is about to be committed. The affidavit and judicial authorization should sufficiently specify the people involved, the facility in question, the specific offenses involved, and the type of information sought to be intercepted. The order should contain a requirement for the minimization of communications not otherwise subject to interception. The order should be effective until the objective of the investigation is achieved or for a period of 30 days, whichever is less. The legislation should contain provisions for recording the intercepted communications and adequate sealing requirements to protect the integrity of the tapes. In addition, the bill should provide for criminal and civil penalities for citizens who intentionally violate the statute.

We strongly oppose, however, the inclusion of any new statutory exclusionary remedy.[1] The admissibility of any evidence with respect to the interceptions would be determined by case law. The bill should also contain a provision allowing the judge to direct a communications common carrier to cooperate and assist law enforcement personnel in the execution of a court order in any way that is appropriate. The provision should further provide the carrier with immunity from civil liability for cooperating and reasonable reimbursement for services rendered.

The bill should also have a provision that covers computer to computer transmissions using telephone lines that do not have a third party communications company involved in the transaction as well as computer to computer transmissions of private communications from facilities not utilizing facilities of interstate commerce. In addition, the new bill should contain emergency provisions similar to Title III where specifically identified supervisory personnel could authorize interception for a limited period of time until application can be made to the court in specified circumstances.

---

[1] Recent privacy enactments such as the First Amendment Privacy Protection Act, 42 U.S.C. 2000 aa, and the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq., contain provisions expressly rejecting an exclusionary sanction or indicating that other remedies afforded are "exclusive", thus impliedly reaching the same result. See United States v Frazin, 780 F.2d 1461 (9th Cir. 1986). We advocate inclusion of a similar provision here.

Unlike Title III, however, the bill should not require that the Attorney General, Deputy Attorney General, Associate Attorney General, or a designated Assistant Attorney General in Washington be the only ones who can authorize the use of the statute. Within the Department we should require supervisory approval in the field by internal regulation.

An order, under the bill, should be obtainable for any offense for which a search warrant could ordinarily be issued. This legislation should also not require that there be a showing that all other investigative procedures have failed or are unlikely to succeed or are too dangerous before an order can be obtained. Additionally, the search warrant or other judicial authorization should be issuable by a magistrate as well as a district court judge of a judge of the court of appeals. A state judge of competent jurisdiction empowered to issue search warrants should also be able to issue a search warrant or other judicial authorization under this legislation. Furthermore, annual reports on the usage of the statute should not be required.

These latter procedures that I have discussed, and that we do not recommend be included in the bill for this type of interception, are appropriate to Title III usage where the level of intrusion with aural communications is greater than the level of intrusion with electronic mail or computer transmissions. The legislation will encompass many of the principal protections of Title III without diminishing the privacy rights of individuals and will be much less burdensome on law enforcement authorities in the conduct of these types of criminal investigations.

B. *Interception or Seizure of Substantive Data Temporarily Stored in a Data Bank of the Communications Common Carrier Prior to Final Transmission to and Receipt by the Recipient*. This covers the time after a specific communication has been sent and while it is in the electronic mail firm's computers but has not been delivered, or has been delivered to the electronic mailbox but has not been received by the recipient. In such a situation, the communication is most like a first class piece of mail and should generally be treated in the same manner. To intercept or seize information of this nature, law enforcement personnel should be required to obtain a search warrant or other judicial authorization predicated upon a sworn affidavit establishing probable cause to believe that a crime has been, is being, or is about to be committed. That is the showing required under Rule 41 of the Federal Rules of Criminal Procedure and should apply here as it does with first class mail. All of the Fourth Amendment requirements for obtaining a search warrant would have to be observed in support of the application. Here too, a magistrate (who is now empowered to issue search warrants) should be able to issue the order as well as a District Judge or a Judge of the Court of Appeals. A state judge of competent jurisdiction who is empowered under state law to issue warrants should be empowered to issue these warrants as well. The warrant should be issuable for any offense under federal or state law for which a search warrant may now be issued. As with Rule 41, this type of warrant should provide for execution within 10 days of the time the order is signed. Since the level of intrusion here is less than in the interception of prospective communications, none of the other Title III type restrictions accorded to the order to intercept prospective transmissions should be applicable to this type of warrant or order. Lastly, a prosecutor in the field supervising an investigation should be empowered to request such an order from the court. Again, this is the same system utilized in seeking a warrant to seize first class mail.

C. Seizure of Substantive Data Temporarily or Permanently Stored in the Files of a Communications Common Carrier After its Receipt. Substantive data that has become part of the records in the files of a communications common carrier should be available to federal investigators during the course of a criminal investigation as a third party document by the service of a grand jury or other statutorily authorized subpoena. Fourth Amendment warrant requirements are inapplicable to this type of document since there is no reasonable expectation of privacy associated with it. This is a well accepted principle of law relating to documents in the possession of third persons and we know of no sound legal or policy reason why it should not apply to these types of documents. To guard against any abuse we could accept a requirement that a supervisory level agent or attorney approve the issuance of the subpoena.

D. Seizure of Transactional Data, Other than Substantive Information of the Communication, Maintained in the Records of the Communications Common Carrier. This type of record includes data retained by the communications common carrier primarily for administrative reasons: i.e., identification of the sender/receiver, date/time of transmission, subscriber, billing information, etc. This is material that is analogous to telephone toll records. The Department believes that the seizure of this type of information is not a "search" within the meaning of the Fourth Amendment, and, therefore, should not require obtaining a search warrant. Law enforcement personnel should be able to secure this information by the service of either a grand jury subpoena or an administrative subpoena served by a law enforcement agency entitled to issue one. We feel that there is no reasonable expectation of privacy with respect to this type of information.

E. Other Provisions. As in Title III, any new legislation regulating the interception of non-aural communications at any stage should contain consent provisions so that either private citizens or law enforcement personnel would be exempt from the statute if they had the prior consent of one of the parties to the communication to make the interception. It is a well settled principle of law that no liability, criminal or civil, would attach under these circumstances.

Finally, any new federal legislation relating to non-aural communications should contain specific authority for the states to enact similar legislation allowing for the state Attorney General or the principal prosecuting attorney in a political subdivision thereof to make application to the court for interception authority. We also recommend that there be a two year delay for the effective date of the new legislation as it applies to the states to allow the states to pass enabling legislation following the guidelines of the federal legislation.

## III. VIDEO SURVEILLANCE

Video surveillance is an additional area in which there is at present no specific statutory authority regulating its use. We believe that special restrictions consistent with Rule 41 procedures and the leading case on the subject, discussed below, should be provided for the issuance of a court order governing the interception of visual images in those situations in which there is a reasonable expectation of privacy on the part of the subjects of the interception.

There are two basic types of video surveillance. One involves the interception of visual images in a fixed location under conditions where the person being viewed would have a reasonable expectation of privacy, i.e., a home or office. The second type involves the interception of visual images (pictures) being transmitted from one location to another, i.e., closed circuit television. The proposed statute should cover both of these.

The leading case authority in this area is United States v. Torres, 751 F.2d 875 (7th Cir. 1984). The Torres case sets forth guidelines for the issuance of a video surveillance order that in the view of the Department adequately protects the rights of citizens and is consistent with the needs of law enforcement in investigating federal violations of law. The Torres court, we note, openly invited Congress to legislate in this area.

Although there is no specific statutory authority for video surveillance, Torres held that a court could issue such a warrant to the extent that certain Fourth Amendment protections, some of which were contained in Title III, were addressed. The court required that there be a search warrant, based upon a sworn affidavit, establishing probable cause to believe a crime has been committed, is being committed, or is about to be committed, and establishing that normal investigative procedures have failed or reasonably appear unlikely to succeed if tried or to be too dangerous. In addition, the warrant must contain a particular description of the facilities involved, a description of the type of images sought to be intercepted, and a statement of the particular offenses to which they relate. Torres also applied the principle that the order must not allow the period of interception to be longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. The court also mandated that a provision for minimizing the interception of images that were not otherwise subject to interception be incorporated in the order. As previously indicated, we feel that these criteria strike a fair balance between the privacy of our citizens and the needs of law enforcement. Current practice in the Department of Justice is to apply the above principles and the teachings of Torres to all requests for closed circuit television involving the invasion of a reasonable expectation of privacy.

For the same reasons as discussed in connection with Title III and the new legislation directed to non-aural communications, legislative authorization of this type should include consent provisions where the interception is made with the prior consent of one of the parties. The consent provision should be applicable to both citizens and law enforcement officers.

In a great majority of cases in which video surveillance is used, it is used in conjunction with an order to intercept aural communications under Title III. In those cases the subject of the interception would enjoy the dual protection of Title III and the new legislation. The Department believes that authority should exist to create a single court order in those cases combining both Title III and video surveillance. Interception of the visual images alone still would enjoy a significant portion of the protection accorded to Title III interceptions.

Finally, due to the degree of potential invasion of privacy involved, the authority to authorize requests to the court for video surveillance orders should be centralized in Washington, D.C. Under current procedures the Attorney General has authorized the Assistant Attorney General, a Deputy Assistant Attorney General, and the Director or Associate Director of the Office of Enforcement Operations to grant the authority to make a closed circuit television request. In practice, this has worked out extremely well and we see no reason to escalate the level of supervision. We recommend that the Attorney General, by statute, be granted the power to delegate this authority through appropriate regulation.

## IV. EXPANDED COVERAGE OF TITLE III

I would like now to turn to several specific proposals to make the current Title III statute even more useful than the last 18 years have proven it to be.

1. The original drafters of Title III sought, out of caution, to minimize its use by specifically limiting its application to designated crimes. There was concern that if its coverage was expanded there may be abuses. The enumerated crimes were those that Congress perceived as being the most significant at the time. The time has come to reevaluate that thinking.

Eighteen years of experience with the statute have demonstrated that abuses have been almost non-existent and that the statutory mechanisms provide ample protection for legitimate privacy interests. In this context, there is no longer valid reason to confine the potential use of Title III to specific felony offenses. In today's society there are a host of other significant crimes where the use of Title III would greatly facilitate the investigations. In fact, from time to time Congress has added new felonies as Title III predicate offenses in almost a haphazard fashion somewhat akin to recognizing the newest most fashionable offense of that year. For these reasons we see no reason that Title III should not be expanded to cover all felonies. In addition, provision should be made to allow Title III electronic surveillance to be used to track down and apprehend federal fugitives. I would like to specifically mention some of the more serious crimes that we encounter today which are not directly covered by Title III although some of them are covered generically by the statute: Threatening or retaliating against a federal official (18 U.S.C. 115); Destruction of an energy facility (18 U.S.C. 1365); Destruction of an aircraft or aircraft facility (18 U.S.C. 32); Aircraft Hijacking (49 U.S.C. 1472); Hostage Taking (18 U.S.C. 1203); Murder For Hire (18 U.S.C. 1952A); Violent Crimes in Aid of Racketeering (18 U.S.C. 1952B); Solicitation to Commit a Crime of Violence (18 U.S.C. 373); Mail Fraud (18 U.S.C. 1341); Illegal Wiretapping (18 U.S.C. 2512); Transportation of Stolen Vehicles (18 U.S.C. 2312); Sale or Receipt of a Stolen Vehicle (18 U.S.C. 2313); Trafficking in Motor Vehicle Parts (18 U.S.C. 2320); Computer Fraud (18 U.S.C. 1030); Fraud involving credit access devices (18 U.S.C. 1029); Escape (18 U.S.C. 75); Instigating or assisting escape (18 U.S.C. 752); and Bail Jumping (18 U.S.C. 3150).

At the very least, the impact of these crimes on society justifies their inclusion in Title III. However, all felonies have an adverse impact and the availability of Title III can make the difference in any felony investigation. Law enforcement officials should, subject to appropriate judicial supervision, have the most effective tools available at their disposal if they are to meet today's challenges in investigating crime and prosecuting criminals.

2. A provision should be included in Title III (as is proposed in H.R. 3378) to allow the Acting Assistant Attorney General in charge of the Criminal Division to authorize a request for a Title III interception and/or eavesdropping warrant. This person is responsible for the operations of the Criminal Division when the Assistant Attorney General is not available, and there is no legitimate reason why this official should not be able to exercise this authority. This authority could greatly reduce delays caused by the absence of the Assistant Attorney General and the need to send Title III applications to substitute Assistant Attorneys General not fully familiar with federal criminal law.

3. A provision should be included in Title III allowing for the interdistrict use of a mobile eavesdropping device or "bug", i.e., where the order is signed in one district to install a bug in a vehicle and the vehicle temporarily goes to another district during the interception period.[2] It should not be necessary, as is the current practice, to obtain an order in each district into which the vehicle travels. The judge in the originating district should be authorized to issue an order that would be effective in all districts into which the vehicle travels during the interception period. This procedure would greatly reduce the burden on law enforcement officials and judges.

4. A provision should be included in Title III that would permit an interception order to be issued targeting an "individual" at whatever facility within the jurisdiction of the court that he or she is using at a given time, as opposed to the authority to intercept only at a particular facility. This would bring the statute in line with the reasoning of Katz v United States, 389 U.S. 347 (1967), that people are protected by the Constitution and not places. Such an amendment could provide significant benefits in the investigation of major drug violators, organized crime figures, and terrorists. Furthermore, in cases involving imminent danger to individuals, such as kidnapping or hostage taking, lives could be saved.

---

[2] A comparable amendment should also be made to Rule 41 to permit interdistrict warrants to install tracking devices.

5. Another administrative provision that should be included in Title III would authorize the use of support personnel under the close supervision of an investigative or law enforcement officer to assist in the monitoring of a Title III. A great deal of the work now being done by law enforcement officers could be taken over by these people leaving the law enforcement officers more time to concentrate on the investigation.

6. A provision should be included in Title III to provide for "after the fact minimization" of foreign language communications where the particular foreign language experts are not reasonably available during the interception period. This provision should give the issuing judge the power to authorize this procedure.

7. We suggest that a provision should be included in Title III providing for a reasonable good faith exception to the exclusionary rule in Title III cases comparable to that which the Supreme Court created in United States v Leon, 104 S. Ct. 3430 (1984) for constitutional violations. A federal offender should not be allowed to escape justice simply because of the objectively reasonable mistake of a law enforcement officer in applying Title III. The judge in each case should have the authority to decide whether or not the mistake was reasonable and thus whether the drastic remedy of excluding reliable evidence

probative of guilt should attach.

8. A provision should be included in Title III to allow for the thirty (30) day period to run from the time the interception begins as opposed to the time when the order is signed. The authorities should have ten (10) days (as is the case with execution of a search warrant under Rule 41) within which to institute the interception. This change would address common difficulties that arise in the installation process while still allowing for the full maximum interception period allowed by the court.

## CONCLUSION

In conclusion, I would like to reiterate that a great deal of thought has been given to the development of these recommendations. We feel that these amendments to Title III and the new legislation for non-aural communications comprise reasonable standards that the Department of Justice and the federal law enforcement agencies could support. Naturally, the details of each proposal require further specification. However, the principles are viable and should provide legislative guidance in these areas for years to come barring unforeseen developments. The Department is committed to working with your staff and with the Senate staff to produce effective legislation.

That concludes my formal remarks, Mr. Chairman. I would be happy to answer any questions you may have.

**Mr. Kastenmeier.** Thank you, Mr. Knapp.

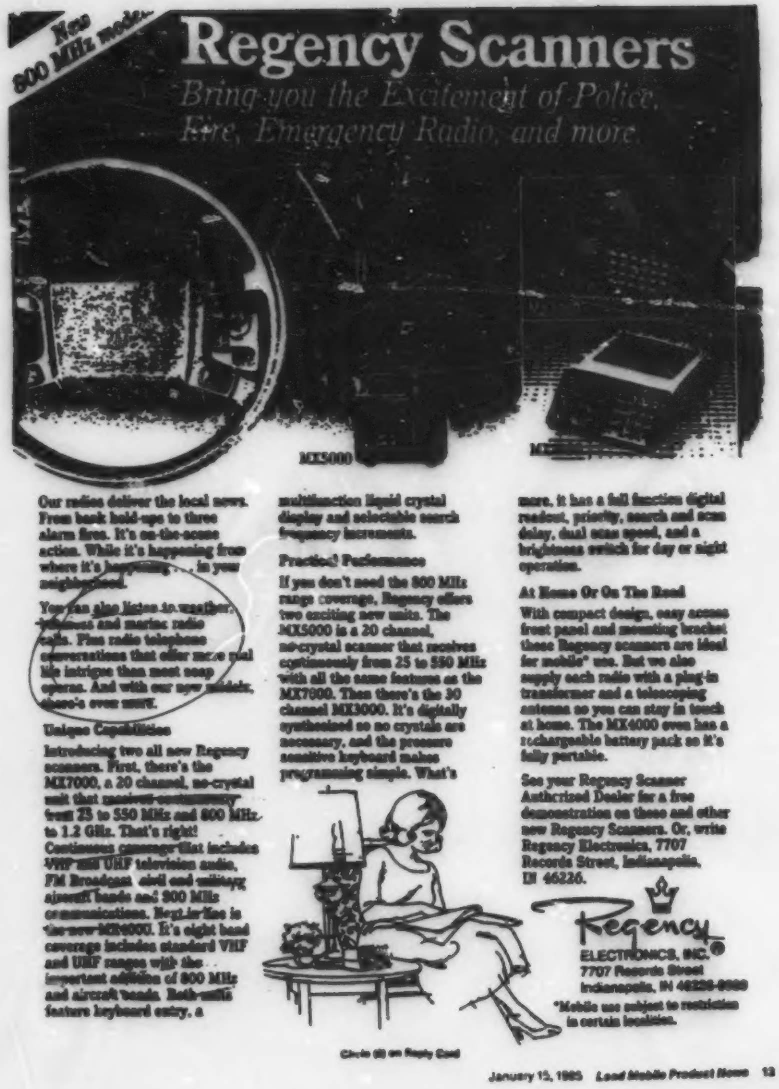
Actually, I think your statement is a good one. I don't know whether we agree on every particular, but I think it is clear that the Department of Justice has given the matter extensive and rather detailed thought, both in terms of policy and in terms of effective implementation. Certainly on that score, I want to commend you, because I think it is by and large a constructive statement.

Without objection, the subcommittee will permit the meeting this afternoon to be covered in whole or in part by radio broadcast or still photography pursuant to the committee rules.

We had recently written the Attorney General to inquire about the current state of the law with respect to interception of cellular telephone calls. My understanding is that it is your position that such interceptions are currently governed by the provisions of Federal wiretap law because they are carried in whole or in part by wire. Is that correct?

**Mr. Knapp.** Certainly where they are covered in part by wire, that would be our position.

**Mr. Kastenmeier.** We also asked about ads—which we have copies of for the record—which explicitly encourage the purchase of scanners for the purpose of overhearing cellular calls.



New 800 MHz models
MX5000

# Regency Scanners

*Bring you the Excitement of Police, Fire, Emergency Radio, and more.*

Our radios deliver the local news. From bank hold-ups to three alarm fires. It's on-the-scene action. While it's happening from where it's happening . . . in your neighborhood.

You can also listen to weather, business and marine radio calls. Plus radio telephone conversations that offer more real life intrigue than most soap operas. And with our new models, there's even more.

**Unique Capabilities**

Introducing two all new Regency scanners. First, there's the MX7000, a 20 channel, no-crystal unit that receives continuously from 25 to 550 MHz and 800 MHz to 1.2 GHz. That's right! Continuous coverage that includes VHF and UHF television audio, FM Broadcast, civil and military aircraft bands and 800 MHz communications. Next in line is the new MX4000. It's eight band coverage includes standard VHF and UHF ranges with the important addition of 800 MHz and aircraft bands. Both units feature keyboard entry, a multifunction liquid crystal display and selectable search frequency increments.

**Practical Performance**

If you don't need the 800 MHz range coverage, Regency offers two exciting new units. The MX5000 is a 20 channel, no-crystal scanner that receives continuously from 25 to 550 MHz with all the same features as the MX7000. Then there's the 30 channel MX3000. It's digitally synthesized so no crystals are necessary, and the pressure sensitive keyboard makes programming simple. What's more, it has a full function digital readout, priority, search and scan delay, dual scan speed, and a brightness switch for day or night operation.

**At Home Or On The Road**

With compact design, easy access front panel and mounting bracket these Regency scanners are ideal for mobile* use. But we also supply each radio with a plug-in transformer and a telescoping antenna so you can stay in touch at home. The MX4000 even has a rechargeable battery pack so it's fully portable.

See your Regency Scanner Authorized Dealer for a free demonstration on these and other new Regency Scanners. Or, write Regency Electronics, 7707 Records Street, Indianapolis, IN 46226.

Regency
ELECTRONICS, INC.®
7707 Records Street
Indianapolis, IN 46226-9989

*Mobile use subject to restriction in certain localities.

Circle 60 on Reply Card

# NEW! Lower Price Scanners

**Communications Electronics,**™ the world's largest distributor of radio scanners, introduces new lower prices to celebrate our 15th anniversary.

## Regency† MX7000-CA

List price $699.95/CE price $379.95/SPECIAL
*10-Band, 20 Channel • Crystalless • AC/DC*
*Frequency range 25-550 MHz. continuous coverage and 800 MHz to 1.3 GHz. continuous coverage.*
The Regency MX7000 scanner lets you monitor military, F.B.I., Space Satellites, Police and Fire Departments, Drug Enforcement Agencies, Defense Department, Aeronautical AM band, Aero Navigation Band, Fish & Game, Immigration, Paramedics, Amateur Radio, Justice Department, State Department, plus thousands of other radio frequencies most scanners can't pick up. The *Regency* MX7000 is the perfect scanner for intelligence agencies that need to monitor the new 800 MHz. cellular telephone band. The MX7000, now at a special price from CE.

## Regency® Z60-CA

List price $379.95/CE price $179.95/SPECIAL
*8-Band, 60 Channel • No-crystal scanner*
*Bands 30-50, 88-108, 118-136, 144-174, 440-512 MHz.*
*Hear Police, Aircraft and the FM Broadcast Bands.*
*The Regency* Z60 covers all the public service bands plus aircraft and FM music for a total of eight bands. The Z60 also features an alarm clock and priority control as well as AC/DC operation. Order today.

## Regency® Z45-CA

List price $329.95/CE price $159.95/SPECIAL
*7-Band, 45 Channel • No-crystal scanner*
*Bands 30-50, 118-136, 144-174, 440-512 MHz.*
The *Regency* Z45 is very similar to the Z60 model listed above however it does not have the commercial FM broadcast band. The Z45, now at a special price from Communications Electronics Inc.

## Regency® RH250B-CA

List price $613.00/CE price $329.95/SPECIAL
*10 Channel • 25 Watt Transceiver • Priority*
The *Regency* RH250B is a ten-channel VHF land mobile transceiver designed to cover any frequency between 150 to 162 MHz. Since this radio is synthesized, no expensive crystals are needed to store up to ten frequencies without battery backup. All radios come with CTCSS tone and scanning capabilities. A monitor and night/day switch is also standard. This transceiver even has a priority function. The RH250 makes an ideal radio for any police or fire department volunteer because of its low cost and high performance. A UHF version of the same radio called the RU150B covers 450-482 MHz. but the cost is $449.00. To get technician programming instructions, order a service manual from CE with your radio system.

## NEW! Bearcat® 50XL-CA

List price $199.95/CE price $114.95/SPECIAL
*10-Band, 10 Channel • Handheld scanner*
*Bands 29.7-54, 136-174, 406-512 MHz.*
*The Uniden Bearcat* 50XL is an economical hand-held scanner with 10 channels covering ten frequency bands. It features a keyboard lock switch to prevent accidental entry and more. Also order part # **BP50** which is a rechargeable battery pack for $14.95, a plug-in wall charger, part # **AD100** for $14.95 and also order optional cigarette lighter cable part # **PS001** for $14.95.

## NEW! JIL SX-400-CA

List price $799.95/CE price $469.95/SPECIAL
*Multi-Band, 20 Channel • No-crystal Scanner*
*Search • Lockout • Priority • AC/DC*
*Frequency range 26-520 MHz. continuous coverage with optionally equipped RF converters 150KHz-3.7 GHz.*
The JIL SX-400 synthesized scanner is designed for commercial and professional monitor users that demand features not found in ordinary scanners. The SX-400 will cover from 150 KHz to 3.7 GHz. with RF converters. Order the following RF converters for your SX-400 scanner: **RF-1030-CA** at $234.95 each for frequency range 150 KHz. - 30 MHz. USB, LSB, CW and AM. (CW filter required for CW signal reception). **RF-5080-CA** at $194.95 each for 500-800 MHz.; **RF-8014-CA** at $194.95 each for 800 MHz.-1.4 GHz. Be sure to also order **ACB-300-CA** at $99.95 each which is an antenna control box for connection of the RF converters. The **RC-4000-CA** data interface at $259.95 each gives you control of the SX-400 scanner and RF converters through a computer. Add $3.00 shipping for each RF converter, data interface or antenna control box. If you need further information on the JIL scanners, contact JIL directly at 213-926-6727 or write JIL at 17120 Edwards Road, Cerritos, California 90701 U.S.A.

## SPECIAL! JIL SX-200-CA

List price $499.95/CE price $157.95/SPECIAL
*Multi-Band - 16 Channel • No-Crystal Scanner*
*Frequency range 26-88, 108-180, 380-514 MHz.*
The JIL SX-200 has selectable AM/FM receiver circuits, tri-switch squelch settings - signal, audio and signal & audio, outboard AC power supply - DC at 12 volts built-in, quartz clock - bright vacuum fluorescent blue readouts and dimmer, dual level search speeds, tri-level scan delay switches, 16 memory channels in two channels banks, receive fine tune (RIT) ± 2KHz., dual level RF gain settings - 20 db pad, AGC test points for optional signal strength meters all for this special price.

## Regency® HX1000-CA

List price $329.95/CE price $189.95/SPECIAL
*6-Band, 30 Channel • No Crystal scanner*
*Search • Lockout • Priority • Scan delay*
*Sidelit liquid crystal display • Digital Clock*
*Frequency range: 30-50, 144-174, 440-512 MHz.*
The new handheld *Regency* HX1000 scanner is fully keyboard programmable for the ultimate in versatility. You can scan up to 30 channels at the same time. The LCD display is even sidelit for night use. Order **MA-256-CA** rapid charge drop-in battery charger for $68.95 plus $3.00 shipping/handling. Includes wall charger, carrying case, belt clip, flexible antenna and nicad battery. Order now.

## NEW! Bearcat® 100XL-CA

List price $349.95/CE price $209.95/SPECIAL
*9-Band, 16 Channel • Priority • Scan Delay*
*Search • Limit • Hold • Lockout • AC/DC*
*Frequency range: 30-50, 118-174, 406-512 MHz.*
The world's first no-crystal handheld scanner now has a LCD channel display with backlight for low light use and aircraft band coverage at the same low price. Size is 1¼" x 7½" x 2¾." The *Bearcat* 100XL has wide frequency coverage that includes all public service bands (Low, High, UHF and "T" bands), the AM aircraft band, the 2-meter and 70 cm. amateur bands, plus military and federal government frequencies. Wow...what a scanner!

Included in our low CE price is a sturdy carrying case, earphone, battery charger/AC adapter, six AA ni-cad batteries and flexible antenna. Order your scanner now.

## NEW! Regency® HX1200-CA

*Now direct channel access feature*
List price $369.95/CE price $214.95/SPECIAL
*8-Band, 45 Channel • No-crystal scanner*
*Priority control • Search/Scan • AC/DC*
*Sidelit liquid crystal display • EAROM Memory*
*Bands: 30-50, 118-136, 144-174, 406-420, 440-512 MHz.*
The new HX1200 scanner operates on 120V AC or 9.6 VDC. Permanent memory backup. Size 2½" x 2" x 7½." Includes wall charger, carrying case, belt clip, flexible antenna and nicad batteries. Order today.

## SPECIAL! Bearcat® DX1000-CA

List price $649.95/CE price $339.95/SPECIAL
*Frequency range 10 KHz. to 30 MHz.*
The *Bearcat* DX1000 shortwave radio makes tuning in London as easy as dialing a phone. Features PLL synthesized accuracy, two time zone 24-hour digital quartz clocks and more. Add $12.00 for shipping.

## NEW! Bearcat® 800XLT-CA

List price $499.95/CE price $299.95/SPECIAL
*12-Band, 40 Channel • No-crystal scanner*
*Priority control • Search/Scan • AC/DC*
*Bands: 29-54, 118-174, 406-512, 806-912 MHz.*
The Uniden 800XLT receives 40 channels in two banks. Scans 15 channels per second. Size 9¼" x 4½" x 12½."

### OTHER RADIOS AND ACCESSORIES

| | |
|---|---|
| Panasonic RF-2600-CA Shortwave receiver | $179.95 |
| Panasonic RF-B300-CA Shortwave receiver | $195.95 |
| RD95-CA Uniden Remote mount Radar Detector | $139.95 |
| RD55-CA Uniden Visor mount Radar Detector | $119.95 |
| BC 20/20-CA Bearcat 40 channel scanner SALE | $224.95 |
| BC 210XW-CA Bearcat 20 channel scanner SALE | $209.95 |
| BC 260-CA Bearcat 16 channel scanner SALE | $194.95 |
| BC 300-CA Bearcat 50 channel scanner SALE | $254.95 |
| BC-WA-CA Bearcat Weather Alert™ | $39.95 |
| DX1000-CA Bearcat shortwave receiver SALE | $339.95 |
| PC22-CA Uniden remote mount CB transceiver | $99.95 |
| PC55-CA Uniden mobile mount CB transceiver | $59.95 |
| 245-CA Regency 45 channel scanner SALE | $159.95 |
| R1060-CA Regency 10 channel scanner | $98.95 |
| MX3000-CA Regency 30 channel scanner | $199.95 |
| XL156-CA Regency 10 channel scanner SALE | $129.95 |
| UC102-CA Regency VHF 2 chan. 1 Watt transceiver | $119.95 |
| RH250B-CA Regency 10 channel VHF transceiver | $329.95 |
| RU150B-CA Regency 10 channel UHF transceiver | $449.00 |
| RPH410-CA 10 ch. handheld no-crystal transceiver | $399.95 |
| BC10-CA Battery charger for Regency RPH410 | $79.95 |
| MA256-CA Drop-in charger for HX1000 scanner | $68.95 |
| MA257-CA Cigarette lighter cord for HX1000 | $19.95 |
| MA917-CA Ni-Cad battery pack for HX1000 | $29.95 |
| EC10-CA Programming tool for Regency RPH410 | $20.00 |
| SMRH250-CA Service man. for Regency RH250 | $20.00 |
| SMRU150-CA Service man. for Regency RU150 | $20.00 |
| SMRPH410-CA Service man. for Regency RPH410 | $20.00 |
| SMMX7000-CA Svc. man. for MX7000 & MX5000 | $20.00 |
| SMMX3000-CA Service man. for Regency MX3000 | $20.00 |
| B-4-CA 1.2 V AAA Ni-Cad batteries (set of four) | $9.00 |
| A-135C-CA Crystal certificate | [illegible] |
| FB-E-CA Frequency Directory for Eastern U.S.A. | [illegible] |
| FB-W-CA Frequency Directory for Western U.S.A. | $12.95 |
| TSG-CA "Top Secret" Registry of U.S. Govt. Freq. | $14.95 |
| TIC-CA Techniques for Intercepting Comm. | $14.95 |
| RRF-CA Railroad frequency directory | $10.00 |
| CIE-CA Covert Intelligence, Elect. Eavesdropping | $14.95 |
| A60-CA Magnet mount mobile scanner antenna | $35.00 |
| A70-CA Base station scanner antenna | $35.00 |
| USAMM-CA Mag mount VHF/UHF ant. w/ 12' cable | $39.95 |
| USAK-CA ¾" hole mount VHF/UHF ant. w/ 17' cable | $35.00 |
| USATLM-CA Trunk lip mount VHF/UHF antenna | $35.00 |

Add $3.00 shipping for all accessories ordered at the same time.
Add $12.00 shipping per shortwave receiver.
Add $7.00 shipping per scanner and $3.00 per antenna.

### BUY WITH CONFIDENCE

*To get the fastest delivery from CE of any scanner,* send or phone your order directly to our Scanner Distribution Center.™ Michigan residents please add 4% sales tax or supply your tax I.D. number. Written purchase orders are accepted from approved government agencies and most well rated firms at a 10% surcharge for net 10 billing. All sales are subject to availability, acceptance and verification. All sales on accessories are final. Prices, terms and specifications are subject to change without notice. All prices are in U.S. dollars. Out of stock items will be placed on backorder automatically unless CE is instructed differently. A $5.00 additional handling fee will be charged for all orders with a merchandise total under $50.00. Shipments are F.O.B. Ann Arbor, Michigan. No COD's. Most products that we sell have a manufacturer's warranty. Free copies of warranties on these products are available prior to purchase by writing to CE. Non-certified checks require bank clearance.

**Mail orders to:** Communications Electronics,™ Box 1045, Ann Arbor, Michigan 48106 U.S.A. Add $7.00 per scanner for U.P.S. ground shipping and handling in the continental U.S.A. For Canada, Puerto Rico, Hawaii, Alaska, or APO/FPO delivery, shipping charges are three times continental U.S. rates. If you have a Visa or Master Card, you may call and place a credit card order. Order toll-free in the U.S. Dial 800-USA-SCAN. In Canada, order toll-free by calling 800-221-3475. Telex CE anytime, dial 810-223-2422. If you are outside the U.S. or in Michigan dial 313-973-8888. Order today.

Scanner Distribution Center™ and CE logos are trademarks of Communications Electronics Inc.
† Bearcat is a registered trademark of Uniden Corporation.
‡ Regency is a registered trademark of Regency Electronics Inc.
AD #011586-CA

Copyright © 1986 Communications Electronics Inc.

**For credit card orders call**
**1-800-USA-SCAN**

COMMUNICATIONS
ELECTRONICS INC.
*Consumer Products Division*
P.O. Box 1045 ☐ Ann Arbor, Michigan 48106-1045 U.S.A.
Call 800-USA-SCAN or outside U.S.A. 313-973-8888

CIRCLE 172 ON READER SERVICE CARD

BEST COPY AVAILABLE

Mr. **Kastenmeier**. What is your view of these ads? Do these ads violate the law?

Mr. **Knapp**. I am reluctant to comment on a specific ad which may or may not constitute a violation. Let me just state a general proposition that it is a violation of 18 U.S.C. 2512, subparagraph (1)(c)(2), where an advertisement promotes the use of a scanner for the purpose of the surreptitious interception of wire or aural communications. So with that statutory guidance in mind, I think you would want to look at the language of a particular advertisement to see if it appears to fit within that.

Mr. **Kastenmeier**. Certainly cellular telephones are very much a part of the scene as an important means of communication. Someone just brought to my attention a copy of the current Time magazine cover. The question is: "Who's This Man Calling? Influence Peddling in Washington." Actually, it is a picture of lobbyist Michael Deaver. Clearly, he is using a cellular phone. So we can conclude that important calls are taking place on cellular telephones. Presumably there is an expectation of privacy—whether that is actually the case or not I do not know.

I have a number of questions but I do want to yield to my colleagues to ask whatever questions they have. The gentleman from California, Mr. Moorhead.

Mr. **Moorhead**. Thank you.

In your statement you maintain the private interception of cellular phone calls should only be illegal if there is both interception and disclosure with a bad purpose, that is, illegal, tortious, or commercial gain.

Is this a statement of how you intend to investigate and prosecute offenders under the bill, or a statement of how the offense should be structured?

Mr. **Knapp**. As I indicated when I gave my remarks a few minutes ago, we are still examining this issue carefully. Initially when we took a look at it, it was our reaction that we clearly don't want to cover the unintentional interception by radio scanners. We thought that perhaps it would be sufficiently effective just to have a statute analogous to what you have for radio communications right now.

However, the cellular industry has asked us to take another look at this problem. What you suggest, perhaps would be a guideline for investigative policy as opposed to the way the bill is drafted, and it is one possible alternative. It is something we have to take a look at. We want a statute that is effective, that is readily understood by the public, and that creates no misconceptions.

Mr. **Moorhead**. It is very clear there are all kinds of mischievous things that you can pick if you have got one of those scanners and you are trying to pick things up—family fights, conversations between someone and their girl friend, confidential information that stockbrokers might be giving out on the phone to a client, corporate heads talking about things that were going to happen within the corporate field that could be used to someone's advantage. Needless to say, it is very difficult to prove commercial gain right away; or even where someone got the information.

Up until recently, there was no cellular technology and the scanners didn't have that frequency on them. Now they are selling the scanners for the sole purpose of picking up these calls. These ads are very explicit that they have got in the newspaper right now. Here is one of them:

> The Regency MX7000 scanner lets you monitor military, FBI, space satellites, policy and fire departments, drug enforcement agencies, Defense Department, aeronautical AM band, aeronavigation band, Fish and Game, Immigration, paramedics, amateur radio, Justice Department, State Department, plus thousands of radio frequencies most scanners can't pick up.

Many of them advertise that you can pick up personal calls and you can be entertained as if you had gone to the adult movie theater. These are people's private calls, and perhaps something should be done to limit the range of these scanners. Admittedly you can't just ban all scanners because they are important for useful purposes.

But our bill tries to get at the basic problem, and that is deliberately trying to intercept these calls. There is no intent to punish someone that happens to pick up something that they shouldn't be listening to and switches to the next band. But it concerns me if you say that we cannot generally try to protect these calls.

There are people that live so far out in the country that they cannot afford the copper wires to take the telephone out that far, and yet with this kind of communication they can have the telephone like everybody else. Are you going to protect them?

Mr. KNAPP. As I indicated, we are going to take a careful look at this specific issue. We feel that a large majority of situations where we were able to prove a violation, you would have the divulgence and a disclosure—and those are the situations that are most aggravated. There is no question we clearly would support such a thing. Whether we go that second step and predicate a violation based on the initial interception itself, I think it is something we want to take a careful look at. But we have agreed to discuss this with the cellular industry and any other concerned parties in the coming weeks, and we will certainly take into consideration your comments and observations.

Mr. MOORHEAD. The bill that has been introduced creates a broad definition of electronic communication, and then proceeds to exempt certain kinds of communication services, like ham operators, police, and fire.

Do you agree that this general approach is better than approaching the subject on a technology basis? Technology by technology.

Mr. KNAPP. I think we probably, in drafting any legislation as indicated in our testimony, want to take a look at the specific technologies first because these devices have legitimate uses as well as illegitimate uses.

Mr. MOORHEAD. In your view, should the development of a new surveillance technology be able to erode the reasonableness of our expectancy of privacy?

Mr. KNAPP. Perhaps it shouldn't, but it does as a practical matter in some situations. That is a concern I expressed in my testimony on cellular. Nevertheless, we factor in the fact that people do have an expectation of privacy, or still a large number of people do. But we feel, so there is no doubt about the state of the law, that cellular should be specifically covered.

Mr. **Moorhead**. I would very much appreciate it if you would come back to the committee when you have gone through this process of formulating positions and directions, because most of the things that we have asked you don't have an answer for yet.

Mr. **Knapp**. I think other than that one issue we do have an answer for just about everything, except for this one issue which I said we would reconsider.

Mr. **Moorhead**. That is the big issue, though, for many of the people out there. There are over 300,000 of these cellular phones now and there will probably be a million within a year. In spite of the fact that part of it goes through the air by radio, people in this country—and perhaps they should know better—expect privacy in their own calls.

I don't think we have got necessarily got the perfect answer for protecting cellular telephone calls. However, in one way or other we value privacy very highly in this country, and we have got to find a way that we can give them as much protection as possible; not 100 percent, it is not available, I would agree with you on that. But we have got to find a way to give them as much as possible.

Mr. **Knapp**. OK. We have made two very specific proposals on this and as to whether we want to take that third-step, I think that is something we will take a very close look at in the next few weeks.

Mr. **Moorhead**. OK.

I yield back the balance of my time.

Mr. **Kastenmeier**. The gentleman yields back his time.

There are a couple of distinctions made which I would like to discuss with you. One is on the current technology of electronic mail messages that are carried between users by a third-party provider, pretty much in the same way that the post office carries mail. One significant difference is that the third-party provider—who could be GTE or Western Union—stores these messages until the recipient is ready to receive them. At that point in time there is a transmission which is stored before delivery.

Would you agree that law enforcement officials should use a search warrant to obtain access to the contents of that stored message? I think you indicated yes.

Mr. **Knapp**. Yes.

Mr. **Kastenmeier**. On the other hand, if an "E" mail provider kept copies of messages for security purposes, you don't feel that law enforcement officials should be required to obtain some form of court order before gaining access to that particular message?

Mr. **Knapp**. Either a court order or grand jury subpoena. If there is an investigation in progress, I think we should be able to utilize the grand jury subpoena as we do for any other type of records.

Mr. **Kastenmeier**. Do you make a distinction before and after delivery, in terms of third-party repository of "E" mail? Do you think there is a distinction to be made? That is to say, should the same process be used with respect to "E" mail which is stored before delivery or a copy which is stored subsequent to delivery?

Mr. **Knapp**. Yes; because I think it probably is predicated on a reasonable expectation of privacy. Before delivery it is still in the process of transmission, it is still a message, it is still a communication, and the search warrant requirement should apply. After it is received, the customer presumably should know or be familiar with what the customs are of the business of the common carrier with which they are dealing and they should be on notice of the fact that they may or may not in a particular situation keep copies where that is the case. If he should know or reasonably should know that they are going to store and keep a permanent record of it, he should not have such a reasonable expectation of privacy as to defeat the proper usage of the grand jury subpoena. That is standard for financial records as well.

Mr. **Kastenmeier**. I guess either of them might have knowledge, that is true. The sender would have caused the message to be sent to the recipient. Of course, in terms of the contents of the message the recipient would not be able to do anything about it—he did not cause the contents, which may be very sensitive with respect to him, to be composed. I wonder if there is a difference between the parties.

In any event, I won't expand on that any further.

In your testimony you have also asked us to distinguish between voice and nonvoice communications. We have recent news clippings which describe new AT&T services which will enable customers to use a combination of telephones and personal computers for various purposes, for various transactions, for example, view financial information on a screen and talk with their brokers at the same time. These communications, I understand, are carried by the same wire. Moreover, at various points in the network these communications are carried in digital form, so that voice and data will in fact be indistinguishable.

With these services and many others like them, is it realistic to make this distinction between the two? Haven't we reached the point where technology has overcome the difference between voice and nonvoice communications?

Mr. **Knapp**. Not for the purposes of determining whether or not you are going to have the specific additional protections of title III over and above what you have for the ordinary search warrant. I think the question is going to be beyond those protections that you have with the ordinary search warrant—is there some practical need for any of the additional protections afforded by title III? And in those situations the answer is no. Although it is said that when we went through and discussed electronic mail I did indicate there were four or five additional protections that were applicable and appropriate, including minimization and including some sort of showing of need. But that is not true. I think you have to look at each technology on a case-by-case basis. Ordinarily, a search warrant requirement of probable cause and order of judicial approval should be sufficient.

In the hypothetical you mentioned, of course, if it is covered partially by wire, communication by wire, title III would apply.

Mr. **Kastenmeier**. In testimony before the subcommittee, ADAPSO suggests the bill be modified to provide additional privacy protection to data stored by remote data processing service providers. What is your view of that suggestion? Or haven't you looked at it, perhaps, and thought about it?

Mr. **Knapp**. Before transmission it is covered by a search warrant and after transmission by grand jury subpoena.

Mr. **Kastenmeier**. So depending on precisely how they wanted to handle it, you may or may not agree with them. I suspect we should encourage them to sit down with you and see whether the current state of the law and your interpretation is for their purposes adequate.

That's all the questions I have.

The gentleman from California.

Mr. **Moorhead**. I just have one more concern here. Most of the cellular phone calls are made to or from fixed installation phones. In other words, somebody will call from an automobile and the person that is on the other end of the wire has a phone in his home—he really expects that to be private.

Mr. **Knapp**. Yes.

Mr. **Moorhead**. I don't think that there is any requirement that the person calling from his automobile inform the person at the other end that the call may be listened to. Yet, in one of these articles it talks about this individual that happens to live in my district that spans——

Mr. **Knapp**. Is that from the Los Angeles Times?

Mr. **Moorhead**. That is from the Los Angeles Times.

With surprising regularity—he also came across fragments of personal telephone calls in which it was obvious that neither party had any idea that someone might be listening. There was none of the sense of audience that often permeates the chatter on a citizen band. They talked about the divorce proceedings, and the narcotics transactions, and the fooling around, and all kinds of stuff.

Some of these things may be legal but you wouldn't want everybody under the sun to know about it.

Mr. **Knapp**. No.

Mr. **Moorhead**. Are you going to say under the law that you are going to make it illegal to make one of the calls from cellular without telling the people on the other end that their call could be made public, that it could be listened to?

Mr. **Knapp**. No.

Mr. **Moorhead**. How are you going to protect them?

Mr. **Knapp**. In fact, as we stated, that is why this article is a very good reason we are advocating that cellular telephones clearly be covered by title III. There is just no question about it, it should be.

Mr. **Moorhead**. I guess we are all anxious that something be done. We need your suggestions, and we need your support, so that we can get a bill through that does protect people from a very important problem.

That is all I have.

Mr. **Kastenmeier**. We thank you very much, Mr. Knapp, for your presentation on behalf of the Justice Department today. We look forward to continuing to work with you on this and other subjects.

Mr. **Knapp**. Thank you very much.

Mr. **Kastenmeier**. Next the Chair would like to call Prof. Clifford F. Fishman. He is a professor of law at the Columbus School of Law, Catholic University of America. I might add that Professor Fishman is a former State prosecutor, author of a leading treatise on wiretapping, and a consultant to the President's Commission on Organized Crime.

Professor Fishman, we have received, of course, a copy of your statement and you are free to proceed as you wish.

## STATEMENT OF CLIFFORD S. FISHMAN, PROFESSOR OF LAW, THE CATHOLIC UNIVERSITY OF AMERICA LAW SCHOOL

Mr. **Fishman**. Thank you very much.

Mr. Chairman and members of the subcommittee:

Striking the right balance between protection of privacy and effective and efficient law enforcement has been a recurring theme in American life and law since the American Revolution. In the past quarter century, advances in technology have enabled investigators to conduct surveillance more effectively and efficiently than their predecessors would have dreamed possible.

At the same time, criminals have also employed the fruits of the technological revolution to make their activities more efficient, more dangerous, more profitable and more difficult to detect. Thus, the challenge of striking the proper balance between law enforcement and privacy is greater today than ever before in our history. I welcome the opportunity to participate in the effort.

I have been asked to comment today about two types of electronic surveillance: pen registers, and electronic tracking devices. I also would be willing to answer questions about some of the issues concerning which Mr. Knapp has just testified.

Mr. Chairman, with your permission, rather than read my recitation of the law dealing with pen registers, I will summarize it basically by saying that the Justice Department, I think correctly, has concluded that it need not get a search warrant in order to obtain a pen register—all they do is get a much easier to obtain order under rule 57(b) from a Federal magistrate. That order need not be based on probable cause nor necessarily even upon reasonable suspicion.

Picking up on page 5 of my remarks now: Is there a need for statutory regulation of pen register surveillance?

It is tempting to answer: "If it ain't broke, don't fix it"—don't impose a regulatory scheme on pen register surveillance unless there is reason to believe that law enforcement has abused the existing lack of regulation.

Even in the absence of abuse, however, regulation may be seen as worthwhile protection against the potential for abuse. If so, the question then becomes whether Congress should legislate the regulatory standards directly, or instead direct the Attorney General to promulgate such regulations and to report periodically to Congress.

Congress took this latter approach when it enacted the Privacy Protection Act of 1980, regulating third-party searches. There is nothing inherently wrong with either approach.

Assuming Congress decides to enact regulatory legislation, the pen register provisions of title II of H.R. 3378 provide a workable and practical scheme. Still, I offer the following comments. Just briefly, I think because a pen register is even less intrusive than a traditional physical search and seizure, U.S. magistrates, who are authorized to issue search warrants, should also be authorized to issue pen registers.

With regard to what factual standard should apply, section 3123(a)(1) would authorize the issuance of a pen register warrant so long as the applicant establishes "reasonable cause to believe . . . that the information likely to be obtained . . . is relevant to a legitimate criminal investigation."

Again, if I may depart briefly, assuming reasonable cause is reasonable suspicion as the Supreme Court has defined that term, that strikes me as an entirely appropriate standard assuming Congress feels it necessary to enact a standard.

Summarizing what is on page 7: Whether it really is necessary that the person who was the subject of a pen register ultimately received notice of that fact, assuming no indictment ultimately arises or results, I have grave doubts. Use of a pen register is very minimally intrusive. It does not reveal who made the phone call; it does not reveal who received the phone call; it does not even reveal whether a phone call was in fact made. All it reveals is that somebody from phone X placed a call—attempted to place a call—to somebody from phone Y. Particularly if the rest of the statute is drafted, requiring a reasonable suspicion before such orders can be obtained, it seems to me that that is enough protection against abuse.

If automatic notice is required, this may jeopardize subsequent investigations as well as imposing, I think, a significant administrative burden upon law enforcement officials who, as we all know, have enough to deal with, to worry about, already.

With regard to electronic tracking devices, on page 7: In 1983 and again in 1984, the Supreme Court examined the fourth amendment implications of the installation and use of electronic tracking devices, or beepers, to assist investigators in following and locating containers of chemicals that the investigators suspected, correctly, were to be used to manufacture or process unlawful drugs. Ironically, the law is in many respects as unsettled now as it was before those cases were decided.

The existing law might best be categorized by each of the stages of beeper surveillance.

First, installation. The court, in *United States* v. *Karo*, held that it does not constitute a search or a seizure for the police to install a beeper in a chemical container so long as the then owner consents, even though the container will soon thereafter be sold to a suspect. Because such consensual installation is neither a search nor a seizure, the Court held, the fourth amendment does not require investigators to obtain a search warrant or other court order.

Second, what I call in-transit monitoring. In *United States* v. *Knotts*, the Supreme Court held that it does not constitute a search and, therefore, no warrant is required, for investigators to use a beeper to follow a container as it is being transported along the public roadways.

The third stage: general vicinity monitoring.

*Knotts* and *Karo* each hold that it does not constitute a search and, therefore, no warrant is required, for investigators to use a beeper to determine the general vicinity to which the beepered object has been taken. In other words, if they lose the object while it is being transported, they can use the beeper to find the neighborhood it is in without it being a search and, therefore, no warrant is required.

The fourth step: private location monitoring.

The *Karo* decision holds that it does constitute a search, for which a warrant of some kind is required, for investigators to use a beeper to determine whether the beepered object is inside a particular private location—a private home or a storage locker, for example.

Is there a need for statutory regulation in this area? The answer basically is yes. The law is extremely unsettled—so much so that investigators and judges often must guess as to what is required, what is permitted, and what is forbidden. The questions that need answers include: Does it constitute a search, that is, is a warrant required, to install a beeper without the owner's consent?

What is the precise dividing line between the warrantless monitoring the Court upheld in *Knotts* and *Karo*, and the kind of monitoring that *Karo* holds must be authorized by a warrant?

Is probable cause required for such a warrant, or will reasonable suspicion suffice? The uncertainty may jeopardize both law enforcement efficiency and individual privacy.

In most respects, H.R. 3378 is an excellent proposal for regulation of beeper surveillance. It spells out appropriate procedures for the issuance of beeper warrants, provides for notice to be given to appropriate individuals after the surveillance is complete, and applies a single factual standard to beeper surveillance at all stages of the process, those now not protected by the fourth amendment, as well as private location monitoring, which is.

The one aspect of title II's treatment of beepers with which I disagree strongly, is section 3123(a)(2), which requires probable cause. Probable cause is an inappropriate standard to apply to beeper surveillance; reasonable suspicion should suffice.

A physical search of a private location is an extremely intrusive procedure. Even if only one object is sought, agents, must enter the location; unless the object is in plain sight once they enter, they must look for it, and in the process of looking, they necessarily and unavoidably see and learn a great deal about those occupying the premises—information that otherwise would remain private. Because such searches are so intrusive, the fourth amendment requires probable cause.

By comparison, private location monitoring of a beeper is minimally intrusive; no physical entry is necessary, and the only fact the agents learn is whether the beeper object is inside. To equate this comparatively minuscule intrusion with a physical search, by requiring the same factual standard for both, is unwise.

Although the Supreme Court has not yet ruled on whether reasonable suspicion suffices to justify private location monitoring, the Court has held in a somewhat different context that where the nature and quality of an intrusion is minor, and the governmental interest in conducting the intrusion is high, reasonable suspicion is the appropriate standard.

What is an accurate description of private location monitoring? Thus, reasonable suspicion is the factual standard against which beepered warrant application should be measured, and I urge the subcommittee to revise H.R. 3378 accordingly.

In conclusion, let me thank you again for the opportunity of appearing before you. I am happy to answer any questions.

[The statement of Mr. Fishman follows:]

STATEMENT OF

CLIFFORD S. FISHMAN

Professor of Law
The Catholic University of America Law School

before the

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

concerning

PEN REGISTERS AND ELECTRONIC TRACKING DEVICES

March 5, 1986

Mr. Chairman and Members of the Subcommittee:

Striking the right balance between protection of privacy and effective and efficient law enforcement has been a recurring theme in American life and law since before the American Revolution. In the past quarter century, advances in technology have enabled investigators to conduct surveillance more effectively and efficiently than their predecessors would have dreamed possible. At the same time, criminals have also employed the fruits of the technological revolution to make their activities more efficient, more dangerous, more profitable and more difficult to detect. Thus, the challenge of striking the proper balance between law enforcement and privacy is greater today than ever before in our history. I welcome the opportunity to participate in the effort.

I have been asked to comment today about two types of electronic surveillance: pen registers, and electronic tracking devices.

## I. PEN REGISTERS

A pen register is a mechanical device, usually installed in a central telephone company facility, that records on paper the numbers dialed from a particular telephone. It reveals only the numbers that have been dialed; it does not enable anyone to hear anything that is being said. It does not reveal who placed the call, nor who received the call, nor even whether the call was completed; all it reveals is that someone used the monitored phone to attempt to reach someone at the number dialed.

Thus, the pen register is a comparatively unintrusive surveillance device. Nevertheless, it can provide valuable information. By providing circumstantial evidence that two suspected criminals may have been in contact with each other, it can help establish the existence of a conspiracy. Moreover, pen register surveillance may help investigators acquire probable cause to obtain a Title III wiretap order on a particular phone, or perhaps persuade them not to seek such an order.

On the other hand, unregulated pen register surveillance could have a deleterious effect on individual privacy. As Justice Marshall has written, "Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts." 1/

## A. EXISTING LAW

In the past two decades Congress has enacted two statutes regulating electronic surveillance, and the Supreme Court has decided two cases involving pen registers; yet, the law is still in a state of uncertainty.

### 1. Title III: the New York Telephone decision

The first statute is Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which requires law enforcement officials to obtain a special interception order before they may monitor wire or oral communications. In 1977, the Supreme Court, in United States v. New York Telephone Company, held that investigators need not obtain a Title III interception order as a prerequisite to pen register surveillance. 2/

### 2. Smith v. Maryland

Two years later, in 1979, the Supreme Court in Smith v. Maryland 3/ held that if a telephone company voluntarily complies with a police request to install a pen register, no Fourth Amendment "search" occurs, and therefore the officers need no court order of any kind. In reaching that decision, the Court made no reference to a statute enacted by Congress the year before: the Foreign Intelligence Surveillance Act (FISA). 4/

### 3. FISA

FISA's primary purpose is to regulate electronic surveillance conducted within the United States to acquire foreign intelligence information. Certain aspects of the statute sweep more broadly, however: FISA's civil and criminal provisions impose sanctions on law enforcement officers who conduct "electronic surveillance" --- including pen register surveillance 5/ --- unless that surveillance is conducted "pursuant to a search warrant or court order ..." 6/

FISA requires national security officials to obtain a FISA order to conduct foreign intelligence surveillance --- whether the surveillance is comparatively unintrusive (e.g. a pen register) or extremely intrusive (e.g. a concealed microphone and camera). It is silent, however, as to what kind of court order would suffice to authorize pen register surveillance for law enforcement purposes.

### 4. Rule 57(b)

At least since 1979, the Justice Department has sought and obtained court orders authorizing pen register surveillance pursuant to Rule 57(b) of the Federal Rules of Criminal Procedure. 7/ That rule provides: "If no procedure is specifically prescribed by rule, [a federal] court may proceed in any manner not inconsistent with these rules or with any applicable statute." Although the application for such an order does contain a brief factual statement as to why the surveillance is sought, the application need not establish probable cause, nor apparently reasonable suspicion, to believe that evidence of criminality will be uncovered.

## B. THE NEED FOR STATUTORY REGULATION

Is there a need for statutory regulation of pen register surveillance?

It is tempting to answer, "If it ain't broke, don't fix it" --- don't impose a regulatory scheme on register surveillance unless there is reason to believe that law enforcement has abused the existing lack of regulation.

Even in the absence of abuse, however, regulation may be seen as worthwhile protection against the potential for abuse. If so, the question then becomes whether Congress should legislate the regulatory standards directly, or instead direct the Attorney General to promulgate such regulations and to report periodically to Congress. Congress took this latter approach when it enacted the Privacy Protection Act of 1980, regulating "third party searches." There is nothing inherently wrong with either approach.

## C. TITLE II OF HR 3378

Assuming Congress decides to enact regulatory legislation, the pen register provisions of Title II of HR 3378 provide a workable and practical scheme. Still, I offer the following comments.

### 1. The issuing authority

Because a pen register is even less intrusive than a traditional physical search and seizure, United States magistrates, who are authorized to issue search warrants, should also be authorized to issue pen register orders.

### 2. The factual standard

Section 3123(a)(1) would authorize the issuance of a pen register warrant so long as the applicant establishes "reasonable cause to believe ... that the information likely to be obtained ... is relevant to a legitimate criminal investigation." The phrase "reasonable cause" is a bit imprecise. Obviously something less than probable cause is intended, and this is entirely appropriate: a pen register intrudes so minimally into privacy that to require probable cause would be legislative overkill.

The Supreme Court has on several occasions upheld searches based upon a "reasonable suspicion"; if that is the standard intended here, then the bill itself, or perhaps your Committee's Report, should say so, to avoid potential confusion. The Court has held that a "reasonable suspicion" exists so long as an investigator can articulate the specific aspects of a situation that justify the suspicion.8/ This burden does not seem excessive.

### 3. Post-surveillance notice; civil liability provision

Section 3126 is modeled after 18 U.S.C. § 2518(8)(d), the Title III notice provision. If Congress determines that post-pen register surveillance notice should be given, the provision appropriately balances the competing interests involved. I question, however, why such notice should be required. Requiring notice adds an additional administrative burden upon law enforcement. Worse, in cases where the surveillance does not lead to criminal charges (a result which is not necessarily inconsistent with the reasonable suspicion that someone using the phone is engaging in criminality), receipt of notice would simply make the suspect more cautious, more circumspect, and more difficult to detect in the future. Measured against these drawbacks, I question whether notice serves a useful purpose in the pen register context. The intrusion into privacy is minimal; the "reasonable cause" (or "reasonable suspicion") and court order requirements adequately assure against abuses by investigators, if assurances are thought to be needed.

## II. ELECTRONIC TRACKING DEVICES

In 1983 and again in 1984, the Supreme Court examined the Fourth Amendment implications of the installation and use of electronic tracking devices, or "beepers," to assist investigators in following and locating containers of chemicals that they suspected, correctly, were to be used to manufacture or process unlawful drugs. Ironically, the law is in many respects as unsettled now as it was before those cases were decided.

## A. EXISTING LAW

Existing law might best be categorized by each of the "stages" of beeper surveillance.

### 1. Installation

The Court, in United States v. Karo, 8/ held that it does not constitute a search or a seizure for the police to install a beeper in a chemical container so long as the then-owner consents, even though the container will soon thereafter be sold to a suspect. Because such "consensual installation" is neither a search nor a seizure, the Court held, the Fourth Amendment does not require investigators to obtain a search warrant or other court order.

### 2. In-transit monitoring 9/

In United States v. Knotts, 10/ the Supreme Court held that it does not constitute a 'search," and therefore no warrant is required, for investigators to use a beeper to follow a container as it is being transported along the public roadway.

### 3. General vicinity monitoring

*Knotts* and *Karo* each hold that it does not constitute a search, and therefore no warrant is required, for investigators to use a beeper to determine the general vicinity to which the beepered object has been taken.

### 4. Private location monitoring

Karo holds that it *does* constitute a search, for which a warrant of some kind is required, for investigators to use a beeper to determine whether the beepered object is inside a particular private location --- a private home or storage locker, for example.

## B. THE NEED FOR STATUTORY REGULATION

Unlike the case with pen registers, the law governing beeper surveillance is extremely unsettled --- so much so that investigators and judges often must guess as to what is required, what is permitted and what is forbidden. The questions that need answers include: does it constitute a search (i.e. is a warrant required) to install a beeper *without* the owner's consent? What is the precise dividing line between the warrantless monitoring the Court upheld in *Knotts* and *Karo*, and the kind of monitoring that *Karo* holds must be authorized by a warrant?

Is probable cause required for such a warrant, or will reasonable suspicion suffice? The uncertainty may jeopardize both law enforcement efficiency and individual privacy.

### C. TITLE II OF HR 3378

#### 1. In general

In most respects, HR 3378 is an excellent proposal for regulation of beeper surveillance. It spells out appropriate procedures for the issuance of beeper warrants, provides for notice to be given to appropriate individuals after the surveillance is complete, and applies a single factual standard to beeper surveillance at all stages in the process, from installation to private location monitoring.

#### 2. Probable cause or reasonable suspicion

The one aspect of Title II's treatment of beepers with which I disagree, strongly, is § 3123(a)(2) (p. 16 lines 10-11). Probable cause is an inappropriate standard to apply to beeper surveillance; reasonable suspicion should suffice.

A physical search of a private location is an extremely intrusive procedure. Even if only one object is sought, agents must enter the location; unless the object is in plain sight once they enter, they must look for it, and in the process of looking, they necessarily and unavoidably see and learn a great deal about those occupying the premises --- information that otherwise would remain private. Because such searches are so intrusive, the Fourth Amendment requires probable cause.

By comparison, private location monitoring is minimally intrusive: no physical entry is necessary, and the only fact the agents learn is whether the beepered object is inside. To equate this comparatively minuscule intrusion with a physical search, by requiring the same factual standard for both, is unwise.

The Supreme Court has held that where the nature and quality of an intrusion is minor and the governmental interest in conducting the intrusion is high, reasonable suspicion is the appropriate standard.11/ That is the situation here, and I urge the Subcommittee to revise HR 3378 accordingly.

In conclusion, let me again thank you for the opportunity of appearing before you.

## FOOTNOTES

1. *Smith v. Maryland*, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting). For a detailed discussion of pen registers, see Fishman, "Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent," 29 *Catholic University Law Review* 557-596 (1980).
2. 434 U.S. 159 (1977).
3. 442 U.S. 735 (1979).
4. Because the pen register surveillance in *Smith* occurred prior to the enactment of FISA, the statute was of course inapplicable to that case.
5. H.R. Rep. (Select Intelligence Committee) No. 1283, 95th Cong., 2d. Sess. 96 (1978), commenting on 50 U.S.C. § 1809. For an analysis of the legislative history of this provision, see Fishman, supra note 1, at 583 n. 129.
6. 50 U.S.C. § 1809(b).
7. See Memorandum, Assistant Attorney General Philip P. Heymann, Chief of the Criminal Division, Department of Justice (December 19, 1979).
8. 104 S.Ct. 3296 (1984).
9. The terms "in-transit monitoring," "general vicinity monitoring," and "private location monitoring" are mine, not the Court's. For a detailed discussion of electronic tracking devices, including an outline of proposed legislation regulating beeper surveillance, see Fishman, "Electronic

Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered," 34 Catholic University Law Review 277-395 (1985).

10. 460 U.S. 276 (1983).

11. United States v. Place, 103 S.Ct. 2637, 2642 (1983).

Mr. **Kastenmeier**. Thank you very much, Professor Fishman, for that very helpful discussion of the law, including, of course, your own suggestions.

In a couple of areas I am inclined to agree, and in a couple of areas I have some concerns. Reasonable suspicion is a standard that should be used for tracking devices. I can understand your rationalization. I guess the Supreme Court left this unsettled in the *Karo* case; and if we end up, in a sense, taking the lower standard, I am afraid it may have other policy implications for the Supreme Court on parallel matters. That concerns me. But I can understand the objection to the higher standard. I think that is a difficult choice.

Mr. **Fishman**. May I comment?

Mr. **Kastenmeier**. Yes.

Mr. **Fishman**. I think one of the reasons perhaps the Court didn't say whether probable cause would be required is it wasn't required to rule on that. My feeling, first, is that if Congress says to the Court that it as a matter of policy thinks that reasonable suspicion should be sufficient, that would have very, very persuasive impact upon the Court when the Court is called upon to decide the constitutionality of a reasonable suspicion warrant.

Let me give you an example of where reasonable suspicion arises but probable cause does not. Let's assume that the police learn that X, a person who we will call X, has just ordered a large quantity of concentrated ammonia from a chemical supply company. Now, there are dozens and dozens of perfectly lawful reasons why somebody might want to obtain a large quantity of concentrated ammonia; and that fact in and of itself may not be suspicious.

But let's further assume the police learn that X's roommate has been arrested two or three times for misdemeanor possession of methamphetamine. Now, ammonia is one of the crucial ingredients in making methamphetamine. It seems to me that when you combine—and let's also assume that X is not known to be an employee of a chemical company—you combine the fact that X is purchasing something which, among other uses, is very important to produce a very dangerous drug, with the fact that he is closely associated with somebody who has a history of at least peripheral involvement with that drug.

Clearly you do not have anything approaching probable cause. But you do, I think, have a reason to suspect that that ammonia might be used to manufacture methamphetamine. If the police can put a beeper in the drum of that ammonia before it is delivered, they can find out easily, effectively, efficiently, and without major intrusion into anybody's privacy, where that drum is taken. If it is taken to some place which is a manufacturing plant that uses ammonia, case closed, no further need for investigation.

If, however, as in the *Karo* case, it is shipped from one place to another over a period of 5 months, either the authorities will have to put in an enormous number of investigative man-hours and perhaps learn nothing, and perhaps lose it and not be able to discover the ultimate source; or they can use a beeper and with minimal resources being spent, and ultimately find out what is being done.

I think that is the kind of example in which reasonable suspicion would permit an effective, efficient, not very intrusive investigation. Whereas to require probable cause would either mean the case dies almost at birth, or the police have to invest in an enormous amount of resources and perhaps only to discover that the activity was lawful all along.

I understand your concerns.

Mr. **Kastenmeier**. I appreciate your position. I think you make a reasonably good case. With respect to notice, I think you were talking about pen register notice. Frankly, notice has always been a difficult proposition, particularly for law enforcement people. They will resist it because they are fearful that they are blowing their case or that they are notifying an organized crime figure in some cases, or a possible spy, of the notice. We have always had to try to tailor those in terms of time, and exceptions, and so forth.

Frankly, it would be simpler, in many cases, not to have the notice provisions, and that may be the case. At least we think that is the case in terms of pen registers.

I think you know what concerns us. The use of these lesser intrusive activities has been growing within the Federal Establishment and possibly without; and they may become so ubiquitous and pervasive that society may really have lost something that we really didn't intend to lose. We ought to in some sense set standards. Part of our problem is the areas you are dealing with and part of it is we have to cope with new technology where the statutory law is silent, and courts are required to rule. Courts have asked for us to write statutory language, because they cannot always answer all questions regarding new technologies by construing old statutes.

But as I say, it is the numerical increase and our concern that something is being lost in these areas: electronic tracking, pen registers, mail covers, and so forth. The curve goes up dramatically in the last few years and presumably will continue.

Let me ask you with respect to an application for a pen register order before a Federal magistrate without having to make the showing that one would need, under FISA.

Are you familiar—I must say I am not—with what happens; what the magistrate considers in terms of granting that authority, practically speaking?

Mr. **Fishman**. I have heard informally that some magistrates apparently insist on reasonable suspicion; some magistrates do not, since there are no statutory standards. In essence right now, each magistrate creates his own rule, which is not necessarily a desirable state of affairs, of course. Obviously, when a magistrate is asked to sign a search warrant, he knows that probable cause is the requirement. But for a pen register, rule 57(b) application, I don't know what individual magistrates do, but since there is no case law and no statutory law, I think it is a magistrate-by-magistrate judgment.

Mr. **Kastenmeier**. That is at least our suspicion. The reason that is not satisfactory is because it enables those who seek such authorization to, frankly, find the magistrate that is in the least trouble in terms of reviewing the application.

Mr. **Fishman**. When I was a prosecutor, I knew that there were people who did that occasionally, never me, of course.

Mr. **Kastenmeier**. Sure, that would be reasonable to expect. The result is that standards are exceedingly low with respect to those

BEST COPY AVAILABLE

grants, presumably, and we may effectively have very little in terms of critical screening judgment. Without statutory standards of somewhat higher level, or at least more explicit, we may have that result.

Should the exclusionary rule provisions of title III include an exception for good faith compliance with a court order?

Mr. **Fishman**. In some respects, I think it always does. For example, if the police make a good faith effort to minimize the interception of nonpertinent conversations, even if their efforts are not entirely successful, courts will permit intercepted communications to be admissible.

I am not sure that I would want the Leon good faith exception doctrine read into title III because title III is so much more intrusive; it is such an intrusive invasion into privacy. Now, if the mistake is purely administrative, a word was left in or crossed out, common sense says, don't let a major investigation go down because an unimportant technicality was omitted.

But on the other hand, if probable cause isn't there, if the Justice Department and the issuing judge both somehow blew it with their determination as to whether or not probable cause for an application existed, given the very, very intrusive nature of a wiretap or a bug, I am not at all sure that the good faith doctrine should apply in that situation.

Mr. **Kastenmeier**. The last question is, and this is sort of a historical question: In your view, how important has title III been in ending what were at least perceived as being potential abuses of law enforcement in the wiretapping area back in the 1968–70 period?

Mr. **Fishman**. I think it has been almost spectacularly successful in that respect. I am not going to claim that there are no illegal police wiretaps being run. But it was my impression as a prosecutor for 8 years, and now for more than 8 years as a law professor, some contacts with the law enforcement community that—whereas, before title III, and in some police departments, it was the norm that you put up an illegal wiretap, claim it was an informant, get a search warrant, and that is the way of doing business.

To the extent that anyone does it that way now, he does it not telling anyone else, because he knows that he faces a Federal felony prosecution if he is found out.

So I think in terms of controlling willful, deliberate abuses by law enforcement, title III has been extraordinarily successful.

Mr. **Kastenmeier**. I am glad to hear that. I would like to think that is the case. I appreciate your expert analysis on that point.

Does counsel have any other questions?

Miss **Leavy**. No, thank you, Congressman.

Mr. **Kastenmeier**. If not, on behalf of the committee, Professor Fishman, I wish to thank you for your testimony; it has been very helpful on this very serious and interesting subject.

Mr. **Fishman**. Thank you.

Mr. **Kastenmeier**. In fact, that not only concludes the hearings today, it concludes the series of hearings on the subject of not only pen registers and electronic tracking devices, but that which affects the new technology—cellular telephones, electronic mail, and so forth.

Indeed, the markup on H.R. 3378, hopefully will be scheduled in the very near future. Until that time, when the committee will meet, the committee stands adjourned.

[Whereupon, at 2:45 p.m., the subcommittee was adjourned.]

BLANK PAGE

# APPENDIX

---

## ELECTRONIC COMMUNICATIONS PRIVACY ACT

### I. Additional Testimony

Letter from John R. Bolton, Assistant Attorney General, U.S. Department of Justice to Hon. Peter W. Rodino (June 6, 1986)

Letter from Edward W. Hummers, Jr. to Hon. Robert W. Kastenmeier (May 12, 1986)

Letter from Jerry W. Cox, Counsel for Dynascan Corporation to Hon. Robert W. Kastenmeier (April 29, 1986)

Letter from Alexander B. Trowbridge, President, National Association of Manufacturers to Hon. Edwin Meese (April 29, 1986)

Letter from R.S. Willis, Vice President, Associated Credit Services, Inc. to Subcommittee on Courts, Civil Liberties and the Administration of Justice (April 25, 1986)

Letter from John R. Bolton, Assistant Attorney General, U.S. Department of Justice to Hon. Robert W. Kastenmeier (April 15, 1986)

Letter from Ward H. White, Vice President, United States Telephone Association to Hon. Robert W. Kastenmeier (April 14, 1986)

Letter from Michelle Meier, Consumers Union to Hon. Robert W. Kastenmeier (April 9, 1986)

Letter from Ted A. Heydinger, Vice President, Government Relations, CBEMA to Hon. Robert W. Kastenmeier (April 9, 1986)

Letter from John W. Roach, President, Tandy Corporation to Hon. Robert W. Kastenmeier (April 9, 1986)

Letter from Travis Marshall, Senior Vice President, Motorola, Inc. to Hon. Robert W. Kastenmeier (April 8, 1986)

Letter from L. Ralph Mecham, Director, Administrative Office of the United States Courts to Hon. Peter W. Rodino (March 25, 1986)

Letter from John Spain, President, Radio-Television News Directors Association to Hon. Robert W. Kastenmeier (March 18, 1986)

Letter from F.W. Gerbracht, Jr., Vice President, Chase Manhattan Bank to Hon. Robert W. Kastenmeier (March 17, 1986)

Letter from Jerry J. Berman, Chief Legislative Counsel, ACLU to Hon. Robert W. Kastenmeier (March 14, 1986)

Letter from William H. Dempsey, President, Association of American Railroads to Hon. Robert W. Kastenmeier (March 14, 1986)

Statement of Edward O. Fritts, President, National Association of Broadcasters before the Subcommittee on Courts, Civil Liberties and the Administration of Justice (March 7, 1986)

Supplemental Statement of ANARC concerning H.R. 3378 "The Electronic Communications Privacy Act of 1985" (February 27, 1986)

Letter from Hon. Robert W. Kastenmeier to Hon. Edwin Meese III, Attorney General of the United States Department of Justice (February 19, 1986)

Letter from Robert A. McConnell, Vice President, CBS Washington, to Hon. Robert W. Kastenmeier (February 4, 1986)

Testimony of Richard L. Brown before the Subcommittee on Courts, Civil Liberties and the Administration of Justice on behalf of Regency Electronics, Inc. (January 30, 1986)

Statement of Richard L. Brown before the Subcommittee on Courts, Civil Liberties and the Administration of Justice on behalf of SPACE (January 30, 1986)

Letter from Richard L. Brown to Hon. Robert W. Kastenmeier ( January 28, 1986)

Letter from Michael Goldsmith, Associate Professor of Law, Brigham Young University to Hon. Robert W. Kastenmeier (January 10, 1986)
Letter from Bruce J. Eggers, Director, Congressional Relations, Ameritech to Hon. Robert W. Kastenmeier (December 17, 1985)
Letter from Richard L. Brown, Counsel to the Satellite Television Industry Association/SPACE to Hon. Robert W. Kastenmeier (December 3, 1985)
Letter from Leslie C. Seeman, General Counsel, The Source Information Network to Hon. Robert W. Kastenmeier (November 21, 1986)
Letter from Christy E. Massie, Counsel, Administration Office of the United States Court to James C. Murr, Office of Management and Budget (October 31, 1985)
Memo from James S. Golden, Southwestern Bell Corporation to Subcommittee on Courts, Civil Liberties and the Administration of Justice (October 31, 1985)
Letter from Hubert F. Owens, General Attorney, Bell South Corporation to the Subcommittee on Courts, Civil Liberties and the Administration of Justice (October 22, 1985)
Letter from Douglass J. McCollum, Attorney, C&P Telephone to the Subcommittee on Courts, Civil Liberties and the Administration of Justice (October 22, 1985)
Letter from Warren G. Austin, General Attorney, Northwestern Bell to the Judiciary Committee (September 30, 1985)
Memo from Jerry J. Berman and Marc Rotenberg, ACLU, to Conferees and Interested Persons (September, 1985)
Letter from Martin T. McCue, Director of Government Relations, Centel Corporation to Hon. Robert W. Kastenmeier (July 17, 1985)
Letter from Jerry J. Berman, Legislative Counsel, ACLU to Hon. Robert W. Kastenmeier (June 26, 1985)
Memo from ACLU Project Staff to Conferees and Interested Persons (June, 1985)
Letter from Lynn W. Ellis, Chairman, IEEE to Hon. Robert W. Kastenmeier (May 24, 1985)
Letter from Mary C. Lawton, Counsel for Intelligence Policy, U.S. Department of Justice (May 20, 1985)
Statement of Uniden Corporation of America before the House Subcommittee on Courts, Civil Liberties and the Administration of Justice
Statement of Pacific Telesis Group for Recommendations for Amendments
Statement of the National Association of Business & Educational Radio Concerning the "Electronic Communications Privacy Act of 1985"
Analysis of H.R. 3378 (Same as S. 1667) "Electronic Communications Privacy Act of 1985" by AT&T
Comments of H.W. William Caming, Attorney and Consultant, upon "Electronic Communications of Privacy Act of 1985"

U.S. Department of Justice

Office of Legislative and Intergovernmental Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

JUN 6 1986

The Honorable Peter Rodino, Jr.
Chairman, Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This letter is to advise you of the Department of Justice's position with regard to H.R. 4952, the Electronic Communications Privacy Act of 1986, which we understand is scheduled for markup on June 10 by the full House Judiciary Committee. This bill makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the members and staff of the Subcommittee on Courts, Civil Liberties and the Administration of Justice, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of H.R. 4952.

Sincerely,

John R. Bolton
Assistant Attorney General

cc: The Honorable Hamilton Fish, Jr.
The Honorable Robert W. Kastenmeier
The Honorable Carlos J. Moorhead

PAUL D P SPEARMAN
(1936-1962)
FRANK ROBERSON
(1936-1961)
DAN J ALPERT
VINCENT J CURTIS JR
ROBERT A DePONT
KATHRYN RILEY DOLE
THOMAS J DOUGHERTY JR
JAMES G ENNIS
RICHARD HILDRETH P C
EDWARD W HUMMERS JR
FRANK R JAZZO
BARRY LAMBERGMAN
PATRICIA A MAHONEY
GEORGE PETRUTSAS
LEONARD R RAISH P C
JAMES P RILEY
MARVIN ROSENBERG
DAVID G ROZZELLE
THOMAS S WALSH

FLETCHER, HEALD & HILDRETH
A PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS
ATTORNEYS AT LAW
SUITE 400, 1225 CONNECTICUT AVENUE, N W
WASHINGTON, D C 20036-2679
(202) 828-5700

RETIRED
RUSSELL ROWELL
EDWARD F KENEHAN
ROBERT L HEALD
FRANK U FLETCHER

COUNSEL
ROBERT M RAWSON

TELECOMMUNICATION CONSULTANT
HON ROBERT E LEE

TELECOPIER NUMBER
(202) 828-5786

WRITER'S NUMBER
(202) 828-5710

May 12, 1986

The Honorable Robert W. Kastenmeier
Chairman, Subcommittee on Courts, Civil
  Liberties and the Administration of Justice
Committee on the Judiciary
United States House of Representatives
Room 2328, Rayburn House Office Building
Washington, D.C. 20515

RE: H.R. 3378 -- Electronic Communications
Privacy Act of 1986

Dear Mr. Kastenmeier:

The Radio Association Defending Airwave Rights (RADAR), a trade association representing radar detector manufacturers, respectfully submits these comments on H.R. 3378. Essentially, RADAR seeks clarification as to the status of radio frequency signal detectors such as radar detectors under this bill.

As RADAR interprets H.R. 3378, radar detection would not constitute unlawful interception of an electronic communication within the meaning of the bill. As an initial matter, radar itself does not appear to be an "electronic communication" as that term is defined (i.e., "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature...."). A radar device employs ultrahigh frequency radio waves which are reflected from an object and then received and analyzed by the device in such a way that the characteristics of the object may be determined. Thus, the radar transmission does not transmit any intelligence per se. Furthermore, even upon subsequent reception and analysis by the receiving unit, it is the characteristic of the signal rather than the "content" of the signal which becomes known.

Section 2510(4) would define "intercept" as "interception of the transmission of the contents...," and "contents" would, in turn, be defined as including "any information concerning the substance, purport, or meaning of that communication." Deleted from this latter definition, as presently set forth in Title 18, would be information concerning the "identity of the parties to such communication or the existence" of that communication.

While an argument can be made that the use of radar itself may result in the conveyance of information, _e.g._, the speed or distance of an object, the detection of radar clearly does not result in the acquisition of any intelligence _per se_. Radar detectors are passive instruments which indicate that certain radio frequencies are being used within a relatively close distance. Detection of radar, therefore, cannot be said to constitute interception of the "contents" of a communication. Radar detectors do not, for example, tell the user the speed at which a car is traveling as it is picked up by radar. The proposed deletion of "identity" and "existence" from the definition of "contents" makes this particularly true. To the extent that the detection of radar may be said to impart any "information," it is more in the nature of conveying the source's "identity" (_e.g._, the police) or the "existence" of such a communication (_i.e._, detection indicates that the frequency is being actively used).

Assuming _arguendo_ that radio frequency signal detectors do fall within the ambit of the bill, RADAR believes they would be encompassed by one of the proposed exceptions. Section 2511(2)(g)(i) would allow any person "to intercept or access an electronic communication made through an electronic communication system that is designed so that such electronic communication is readily accessible to the general public." Given the proliferation of these instruments, radar or any type of radio frequency signal would seem to be a "readily accessible" communication, although that term is not defined in the bill. Moreover, Section 2511(2)(g)(ii)(II) would specifically provide for an exception for police radio communications which are readily accessible to the general public. Radar may be categorized under this exception as well.

In light of the foregoing, RADAR urges that clarifying language be added to either the bill or the bill's legislative history to the effect that use of radio frequency signal detectors does not constitute unlawful interception of an electronic communication. RADAR suggests that an appropriate place for such language would be under Section 2511 which contains the bill's exceptions.

Very truly yours,

Barry Lambergman

Edward W. Hummers, Jr.
Barry Lambergman
Counsel for RADAR

BL:ba:
cc: David Beier, Esquire
Deborah Leavy, Esquire
Ms. Janice Lee

SIDLEY & AUSTIN
A PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS
1722 EYE STREET, N.W.
WASHINGTON, D.C. 20006
TELEPHONE 202: 429-4000
TELEX 89-463

ONE FIRST NATIONAL PLAZA
CHICAGO, ILLINOIS 60603
312: 853-7000 TELEX 25-4364

2049 CENTURY PARK EAST
LOS ANGELES, CALIFORNIA 90067
213: 553-8100 TELEX 18-1391

[illegible] MADISON AVENUE
NEW YORK, NEW YORK 10022
212: 418-2100 TELEX 97-1696

38 ST. JAMES'S SQUARE
LONDON, SW1Y 4JH, ENGLAND
44-1: 930-5596 TELEX 21781

P.O. BOX 190
MUSCAT, SULTANATE OF OMAN
968: 722-411 TELEX 5264

P.O. BOX 4610
DEIRA, DUBAI-U.A.E.
9714-243194 TELEX 47216

5 SHENTON WAY
SINGAPORE 0106
65 224-5000 TELEX 28754

P.O. BOX 8850
RIYADH, SAUDI ARABIA
966-1-463-4160 TELEX 204947

SIDLEY & AUSTIN & NAGUIB
AHMED NESSIM STREET, 3
GIZA, CAIRO, EGYPT
202 720-496 TELEX 93780

April 29, 1986

The Hon. Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil
Liberties and the Administration
of Justice
Committee on the Judiciary
United States House of Representatives
2137 Rayburn House Office Building
Washington, D.C. 20515

Re: H.R. 3378, "The Electronic
Communications Privacy
Act Of 1986"

Dear Mr. Chairman:

Dynascan Corporation, a Chicago-based supplier of telecommunications and consumer electronics products, asks that the Subcommittee consider the attached comments before it decides whether to report H.R. 3378 to the full Judiciary Committee.

Dynascan's principal objection to the bill, as presently drafted, is that it would mislead users of cellular and similar types of telephone systems into believing that the law actually protects their privacy. Dynascan would support the bill if it prohibited use and divulgence, rather than interception, of the contents of conversations carried over the public airwaves.

If there are any questions about Dynascan's comments, or if I can be of assistance, I am at the disposal of the Subcommittee and its staff.

Sincerely,

JWCox

Jerry W. Cox
Counsel for Dynascan Corporation

cc: Members of the Subcommittee
on Courts

# COMMENTS OF DYNASCAN CORPORATION
# ON H.R. 3378
# "THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986"
# BEFORE THE SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE
# COMMITTEE ON THE JUDICIARY
# UNITED STATES HOUSE OF REPRESENTATIVES

APRIL 29, 1986

Dynascan Corporation, a leading supplier of telecommunications and consumer electronics products based in Chicago, Illinois, strongly opposes H.R. 3378 as presently drafted and requests that the bill not be reported to the Judiciary Committee. Dynascan would not object to illegalization of the use and divulgence of information gleaned from conversations using cellular telephones and other technology that did not exist when Congress passed the Omnibus Crime Control and Safe Streets Act of 1968. However, the proposal to outlaw simple interception of conversations would undermine, rather than enhance, the privacy of those who use the new technology.

In each draft we have seen, H.R. 3378 outlaws the interception of unencrypted signals being carried over the public airwaves. Dynascan opposes this provision because it ignores two fundamental facts of physics and human nature. First, whenever someone broadcasts his conversation over the airwaves, it is possible for others to listen. Unencrypted broadcast signals can be intercepted inadvertently, often with nothing more sophisticated than a transistor radio. In fact, some car telephone systems cannot be used effectively unless the caller deliberately listens for the end of a conversation.* Second, if it is easy to listen to other people's conversations, people will do so.

As one of the earliest innovators in the design of cordless telephones and a leading designer of citizens band transceivers and other communications devices, Dynascan recognizes that users sometimes forget the difference between traditional wire communications and newer systems that utilize the airwaves. The Federal Communication Commission therefore requires all cordless telephone manufacturers to remind consumers that their words are being broadcast by placing a prominent warning label on the equipment. Instead of emphasizing the vulnerability of the conversation to interception, however, H.R. 3378 attempts to create an expectation of privacy where none can realistically exist. By outlawing "interception of the transmission of the contents" of such communications, H.R. 3378 would give callers a false sense of security. Congress would thereby mislead the public and discourage technological advances that would provide actual protection. Until encryption is more widely available, however, the FCC's policy of educating consumers is far more realistic because it does not create an aura of privacy around conversations that are, by their physical nature, anything but private.

---

* Where cellular technology is uneconomical, car telephone systems function much like the old-fashioned rural party line. A user cannot know whether the channel is clear without listening.

Although the exemption in recent drafts of H.R. 3378 for those who "intercept or access" a signal from a system that makes a conversation "readily accessible to the general public" is well-intentioned, the provision fails to allay Dynascan's concerns for two reasons. First, nothing in H.R. 3378 indicates what is "readily accessible to the general public." Second, the revised draft would still establish an unrealistic general rule illegalizing interception of unencrypted, unsecured signals. To outlaw all such interception, and then try to carve out exceptions to the general rule, would unduly complicate the legislation and confuse its meaning.

Dynascan has no objection to a rule against use or divulgence of information obtained from conversations carried over the airwaves. Interception of such conversations will continue to be a fact of life regardless of whether H.R. 3378 becomes law, but Congress should not make matters worse by engendering a false sense of security among those who fail to remember that their words are being broadcast. Furthermore, enforcement of such a rule will be difficult enough without saddling law enforcement authorities with the additional burden of prosecuting casual listeners.

We regret our inability to support H.R. 3378 as currently drafted. We would be pleased to work with the Members and the Subcommittee staff to help develop a bill we can wholeheartedly support.

National Association
of Manufacturers

ALEXANDER B. TROWBRIDGE
President

April 29, 1986

The Honorable Ed Meese
Attorney General
U.S. Department of Justice
Washington, D.C.  20530

Dear Ed:

On Wednesday, April 30, the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House of Representatives Committee on the Judiciary is scheduled to markup legislation of great importance to our membership and to the business community in general. The legislation is H.R.3378, the Electronic Communications Privacy Act of 1985.

The Telecommunications Task Force of the National Association of Manufacturers has considered the impact that H.R.3378 will have on the effective operation of modern business procedures and has urged the Subcommittee to act quickly and positively on this bill. While other trade associations have also endorsed the Electronic Communications Privacy Act as necessary and beneficial, NAM's Telecommunications Task Force represents the general business communications user. In addition, the Task Force contains representatives from the equipment manufacturing and service provider sectors.

The reason for this broad support is that the statutory protections for communications privacy have not kept pace with the rapid advancement of technology. These developments in technology have allowed American corporations to remain competitive with foreign manufacturers by introducing efficiencies into the methods of communications.

As you know, Title III of the Omnibus Crime and Safe Streets Act of 1968 is the primary statute which both protects the privacy of communication and allows for legitimate law enforcement investigations to intercept these communications. However, it is necessary that this law be updated since the language of the statute limited its application to oral and aural communications utilizing wire transmission. Modern business operations demand an increasing use of telecommunications, from videoconferencing to cellular telephone calls to data communications through computers, as well as the use of remote computing services (which includes "electronic mail").

1776 F Street, N.W.
Washington, D.C. 20006
[illegible]

The NAM recognizes that there are law enforcement concerns about this legislation, but does not view these as irreconcilable with the goal of protection of privacy of modern -- and future -- communications.

NAM, and the business community in general, are more than willing to work with your Department to arrive at statutory language acceptable to all parties. We are certainly aware of the time and energy which Justice Department officials have exerted on this legislation. On behalf of the membership of NAM, however, I would like to emphasize that this is a matter of extreme interest and concern to our members and that your personal attention in helping to resolve these difficult differences between efficient business procedures and legitimate law enforcement activities would be appreciated.

Thank you for your attention and consideration.

Sincerely,

Sandy Trowbridge

Alexander B. Trowbridge
President
National Association
of Manufacturers

cc: Mr. Steve Trott
Mr. James Knapp

**Associated Credit Services, Inc.**

A SUBSIDIARY OF
COMPUTER SCIENCES CORPORATION

Corporate Offices
652 E. North Belt, Suite 400
Houston, Texas 77060
713/878-1900

April 25, 1986

House Judicial Subcommittee
Courts, Civil Liberties, and Administration of Justice
2137 Rayburn House Office Building
Washington, D. C. 20515

Associated Credit Services, Inc. (Pinger System) support the principals embodied in HR 3378, The Electronic Communications Privacy Act. We believe this legislation will provide the additional protection against computer crime our industry needs.

Sincerely,

R. S. Willis
Vice President

RSW:cca

U.S. Department of Justice

Office of Legislative and Intergovernmental Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

15 APR 1986

The Honorable Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties
  and The Administration of Justice
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This letter is designed to augment the Department of Justice's March 5, 1986, testimony before the Subcommittee on Courts, Civil Liberties and the Administration of Justice with regard to H.R. 3378, the Electronic Communications Privacy Act. At that hearing, Congressman Moorhead asked the Department's representative, Deputy Assistant Attorney General James Knapp, to reconsider the position set forth in the Department's written Statement with respect to the private interception of cellular telephone communications. As you may recall, the Statement indicated that, although the Department was prepared to "accept legislation that ... would require Title III authorization for law enforcement officers to intercept either the wire or radio transmission portion of cellular communications", citizen scanning for recreational purposes should not incur liability for interception alone but rather -- by analogy to the Communications Act of 1934 -- only where the citizen "both intercepts and divulges the communication under circumstances in which the interception and divulgence are illegal, tortious, or for commercial gain." Mr. Knapp stated at the hearing that this aspect of the Department's written submission would be reconsidered and that the Department would make a final recommendation to the Subcommittee after meeting with various interested parties over the next few weeks.

This letter will serve to advise the Subcommittee of the results of our reconsideration of the cellular private interception issue, as well as to suggest some additional ideas relating to the legislation before the Subcommittee.

As promised, the Department of Justice since March 5 has held a series of discussions with representatives of the cellular telephone industry as well as the manufacturers of scanners and other interested persons or groups. These meetings were frank and probing and contributed significantly to our understanding of the issues. The question at issue with regard to whether the unauthorized private interception of cellular telephone communications should be criminalized is a difficult one for the Department inasmuch as it involves problems both of assessing the extent of privacy intrusion inherent in such interception as well as problems of enforcement of any prohibition. In this latter regard, Congress should be under no illusion, if offenses in this area are created, that the Department, because of the difficulty of such investigations, would be able to bring a substantial number of successful prosecutions.[1]

Nevertheless, with those caveats, the Department has concluded that its originally stated position with regard to the private interception of cellular telephone conversations should be modified. Because we believe that persons' conversations over cellular telephones should enjoy the protections of federal law, as they do today if carried in part over wire, we are prepared to support legislation that would amend Title III's definitional provisions to specifically cover the radio component of cellular communications. This would clearly bring communications over cellular telephones within the ambit of Title III.

However, our consideration of this issue has also led us to reevaluate the present penalty structure of Title III, which as you know in section 2511(1)(a) makes any willful interception of a wire or oral communication a five-year felony. In our judgment, this penalty, for a first and unaggravated offense of simple interception, is too severe.[2] We think fairness and enforcement would be enhanced if a first offense of simple interception of the radio portion of a cellular communication were to be a petty offense.[3] The existing felony penalties would continue to apply for interception accompanied by divulgence or use for a tortious, illegal, or commercial purpose, as well as for a second or subsequent simple interception offense. In our view, criminalization of the private interception of cellular communications (which would require proof that the defendant was aware that the communication being intercepted was of a protected kind and not, for example, a conversation over a cordless telephone), coupled with the above-suggested refinements in the penalty structure for Title III interception violations, represents the most appropriate balancing of the competing interests in this complex field.

---

[1] With respect to the degree of privacy or security enjoyed by the radio portion of cellular communications, we have been advised by the Federal Communications Commission that technology has advanced to the point that unencrypted radio transmissions cannot in fact be protected from eavesdropping. That agency is therefore concerned that legislation penalizing the interception of unencrypted radio transmissions may create unmerited expectations of privacy within the general public.

[2] Our comment is confined to subsection (1)(a) and is not intended to suggest changing the applicable penalties for offenses under subsections (1)(b),(c), or (d). Nor do we suggest changing the penalty for interception of the wire portion of any communication.

[3] In addition, the legislative history of the bill should make clear that such sanctions apply only to intentional interceptions, not inadvertent overhearings of a protected radio transmission.

We also recommend consideration by the Subcommittee of an injunction provision as an additional form of remedy for prospective or ongoing breaches of Title III. As part of the Comprehensive Crime Control Act of 1984, Congress enacted 18 U.S.C. 1345, which for the first time permits the United States to obtain an injunction against fraudulent practices under the wire, mail, and bank fraud statutes. In our view, a similar injunction provision in the context of Title III would be useful, either pending prosecution or in a suitable instance as an alternative thereto, as a mechanism for curtailing ongoing practices that threaten the privacy interests protected by that statute.

The Department appreciates the opportunity to provide you with our views on this important matter and we look forward to working with you and the Subcommittee staff in the development of appropriate legislation.

Sincerely,

John R Bolton

John R. Bolton
Assistant Attorney General

USTA

**United States Telephone Association**
900 19th Street, N.W., Suite 800
Washington, D.C. 20006-2102
(202) 835-3100

April 14, 1986

The Honorable Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties
and the Administration of Justice
Committee on the Judiciary
2137 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Kastenmeier:

I am writing concerning a bill now pending in your subcommittee, HR 3378, which would amend the Omnibus Crime Control and Safe Streets Act of 1968. We understand that these amendments are intended to ensure that there is consistency in the application of the law to new communications technologies that have emerged since 1968, and also in the application of the law to entities offering those services and technologies.

The United States Telephone Association (USTA) is the trade association of local telephone companies. Its membership exceeds 1100 companies, and its companies supply 99% of the nation's telephone lines.

USTA member companies have been working with your subcommittee throughout the year to help refine HR 3378. We know our member companies want to find a legislative balance that accommodates new technology, protects their customers' reasonable expectations of privacy, yet permits law enforcement agencies to properly carry out their responsibilities.

In line with USTA member support in principle of the goals of HR 3378, USTA pledges its cooperation in the drafting of a bill its members can wholeheartedly support. The subcommittee is well on its way to that goal, and has addressed particular concerns of the telephone industry. As you well know, local telephone companies are directed to act

BEST COPY AVAILABLE

in certain ways with respect to authorized investigations and other activity under the Act. This higher level of interaction requires more caution by USTA and its member companies in reviewing legislative proposals that might affect these relationships. We hope the subcommittee will remain sensitive to our members' concerns in this regard.

USTA does not formally endorse any legislative proposal until its Board of Directors has had an opportunity to fully analyze its implications. That process has not taken place because the bill has been subject to amendment. However, based on our member company involvement, USTA can go on record as being supportive of the current goals of the bill and express support for your efforts to clarify the law. Our USTA staff, including our General Counsel, will remain available to you on an ongoing basis for consultation on HR 3378.

Very truly yours,

Ward H. White
Ward H. White
Vice President
Govt. & Public Affairs

Copy to:
✓D. Leavy

Consumers Union
Publisher of Consumer Reports

[illegible]

April 9, 1986

The Honorable Robert Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties, and
the Administration of Justice
2328 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Kastenmeier:

I understand that the subcommittee you chair will mark-up H.R. 3378, the "Electronic Communications Privacy Act of 1965," tomorrow. We endorse the major thrust of the bill, but we do have two concerns that we hope you will address.

First, the bill, in its present form, may undo some important privacy protections that already exist. This may come about because of the language of sections 2511(3)(B) and 2702(b), as they are added by the bill. For example, section 2702(b) presently reads: "A person may divulge the contents of a communication-- . . ."

This subsection then goes on to enumerate the circumstances under which divulgence can occur without impunity. Because this subsection is written so broadly, it could easily be interpreted to supercede any existing laws that otherwise would not allow disclosure under the circumstances enumerated. One law that could be superceded is the Fair Credit Reporting Act, which prohibits the disclosure of credit information except under specific circumstances.

I do not believe that you intend to supercede existing privacy protections in this bill. A simple amendment that clarifies that subsection 2702(b) only limits subsection 2702(a), and not current privacy laws, would totally address our concern.

We also hope that the committee report will make it clear that "knowingly divulg(ing)" the contents of a communication includes divulgences involving willful blindness. In other words, a service provider should be prohibited from using security systems that recklessly allow unauthorized access to the contents of a communication. Although a provider may not "knowingly" divulge the information, the report should make it clear that civil liability is incurred if information becomes available to unauthorized persons because the security protections were inadequate.

Washington Office
Suite 520, 2001 S Street, Northwest · Washington, D.C. 20009 · (202) 462-6262

We commend you for addressing the concerns of both the industry and the public regarding the privacy problems posed by electronic communications, and we hope to work with you further in this area.

Yours truly,
Michelle Meier
Michelle Meier

cc: Deborah Leavy

CBEMA

April 9, 1986

Hon. Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties
 and the Administration of Justice
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Kastenmeier:

I am writing to provide CBEMA's views on H.R. 3378, which we understand will be marked up by your Subcommittee in the near future. CBEMA enthusiastically endorses the concept of legislation which will extend safeguards against unauthorized access to all forms of electronic communications.

Our interest in this area is obivious. CBEMA is the trade association of manufacturers and assemblers of information processing, business and communications products, supplies and services. Our 39 member companies employ more than 1.6 million people worldwide.

CBEMA supports your efforts to extend traditional constitutional protection to all electronic communications -- both voice and data. In particular we support:

- o the extension of safeguards against interception from voice transmission to virtually all electronic communications;
- o the provision to provide civil and criminal penalties for unauthorized access, allowing the individual to seek civil damages against the guilty parties when their rights have been violated;
- o the concept of minimizing intrusiveness and maximizing fairness in record-keeping systems;
- o the careful balancing of interests in the provisions dealing with permissible interception by law enforcement agencies.

There are, however, three issues raised by the draft bill which we feel need further clarification.

Computer and Business Equipment Manufacturers Association 311 First Street, N.W., Suite 500, Washington, D.C. 20001 (202) 737-8888

The "exceptions" listed under Section 101 (b) do not contain a specific exemption for data interception authorized by the system provider as part of contract maintenance of the system facilities. Frequently, business equipment maintenance agreements provide for remote diagnosis of malfunctions via telecommunication facilities, in which an actual message is intercepted by or disclosed to the maintenance provider, in order to determine the cause and extent of the malfunction. Report language should be offered to exempt these authorized interceptions and disclosures.

With respect to exclusions set out in Section 101 (b)(2), a number of CBEMA members are concerned with the draft bill's approach. Non-carrier private systems incorporating radio transmission by terestrial microwave or satellite, where the facilities are owned and exclusively used by a private system operator, would appear to be exempt from coverage under the present draft. These private systems, which include many corporate internal networks, would benefit from the draft language on unlawful interception. However, the wording of Section 101 (b)(2) suggests that unless the data transmission is made inaccesible, it is available to anyone technically capble of reception. We recommend that an amendment or report language clarifying this ambiguity be added.

We strongly endorse the present draft's treatment in Title II of "data in storage" as a substantial improvement in the protection afforded to such data. We wish to point out, however, that a third type or "state" of information exists; this is "data in process", where the transmission may have already occured, but the data does not yet reside in storage. "Data in process" should be accorded the same high level of protection from both unauthorized private and official investigative interception which is currently provided business records in a locked filing cabinet. We believe this goal could adequately be addressed by report language which expressly incorporates the concept of data in process.

Again, Mr. Chairman, we thank you for your leadership and hope we can continue to work together as this legislation develops.

Sincerely,

Ted Heydinger

Ted A. Heydinger
Vice President,
Government Relations

**Tandy Corporation/Radio Shack**

Executive Offices 1800 One Tandy Center Post Office Box 17180 Fort Worth, Texas 76102 Telephone (817) 390-3700

John V. Roach
President
Chief Executive Officer
Chairman of the Board
390-3317

April 9, 1986

VIA MESSENGER

The Honorable Robert W. Kastenmeier, Chairman
2137B Rayburn House Office Building
Washington, D.C. 20515

Re: H.R. 3378

Dear Congressman Kastenmeier:

Tandy Corporation/Radio Shack is the largest retail distributor of consumer electronic products -- including cellular telephones and radio-band scanners -- in the United States. It is also one of the largest manufacturers of these products. As such, Tandy has an important interest in the work of the Judiciary Committee as it proceeds to consider H.R. 3378, the Electronic Communications Privacy Act of 1986.

As expressed more fully in Mr. George Kuhnreich's testimony on January 30, 1986, Tandy believes that cellular telephone calls should be considered more akin to wireline telephone calls than to other radio transmissions, and thus extended the same legal protection afforded to wireline calls. Tandy thus strongly supports the extension of privacy protection to cellular telephone calls as well as protecting the right of users of radio-band scanners to receive communications in which there has never been any perception or expectation of privacy (e.g., amateur radio, CB, police and public safety, and ship-to-shore communications).

We urge you to insure that these important interests are recognized in any legislation resulting from your consideration of H.R. 3378.

Very truly yours,

John V. Roach
John V. Roach

MOTOROLA INC.

April 8, 1986

The Honorable Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties and
  the Administration of Justice
Committee on the Judiciary
United States House of Representatives
2137 Rayburn House Office Building
Washington, D.C. 20515

RE: HR 3378; Electronic Communications Privacy Act

Dear Mr. Chairman:

Motorola, Inc., respectfully submits the following comments on the above entitled matter.

Motorola, Inc., is one of the world's leading manufacturers of telecommunication equipment. Among its many products are cellular telephone systems, private and common carrier land mobile radio systems, mobile and portable data communications equipment and radio paging systems. Motorola's Corporate Headquarters is Schaumburg, Illinois; however, Motorola manufactures in eleven states and various foreign countries. Motorola's equipment is used in all forms of business, industry and public safety. One example you are familiar with is the House of Representatives paging system.

Motorola supports the intent of HR 3378. As we understand it, you intend to provide privacy for voice and data communications where a reasonable person would expect to have privacy. At the same time, you do not intend to affect hobby uses or amateur radio or those business uses which require monitoring of a radio channel in order to effectively provide communications.

Motorola's major concern with HR 3378 lies with any possible effect it could have on the normal use of a land mobile radio system licensed by the Federal Communications Commission (FCC) in the Private Land Mobile Radio Services. The dramatic growth of mobile radio to increase efficiency at lower costs has caused the demand for spectrum to exceed the meager supply available. As a result, land mobile radio users must share frequencies. This sharing requires that any user monitor the frequency to insure that it is clear prior to transmitting. In addition, base station operators may monitor the channels in order to perform maintenance, to control the system, and to correct interference situations.

Licensees in the Private Radio Service know from the outset that assigned frequencies are non-exclusive. Therefore, they do not have the expectation of privacy envisioned in your legislation. NABER has described the unique operational characteristics of these private services. Motorola concurs with the points made in the NABER statement.

Government Relations: 1776 K Street, N.W., Suite 200, Washington, D.C. 20006    (202) 862-1500

On March 4, the Utilities Telecommunications Council (UTC) filed its comments on this legislation. UTC recommends an amendment to exempt private land mobile communications. (See p. 5 of UTC letter). Motorola would support such an amendment.

The UTC, on page six of its comments, also suggests that the exemption for electronic surveillance be broadened to include "power generating and other industrial plant locations." Electronic surveillance may also be used in an office building, public or private, as an economical means of preventing ready access by the general public to certain portions of the building. The legislation should not limit this method of monitoring unauthorized access to portions of a building.

As a major manufacturer of cellular mobile telephone equipment, Motorola concurs that the users of cellular mobile and portable telephones have a legitimate expectation of privacy. This expectation is the same as we have on our business or personal telephones which use wires. The fact that a cellular telephone uses radio frequencies to transmit a message, rather than wire, should make no difference. A telephone call, regardless of transmission medium, should be treated as a telephone call.

Motorola is considering manufacturing encryption equipment for cellular phones. However, we do not believe that the ordinary user, expecting privacy, should be required to expend resources to purchase a device to insure the reasonable expectation he had when he purchased or leased his cellular telephone.

Motorola appreciates the opportunity to comment on this legislation.

Sincerely,

Travis Marshall
Senior Vice President
Director, Government Relations

L. RALPH MECHAM
DIRECTOR

JAMES E. MACKLIN, JR.
DEPUTY DIRECTOR

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

WASHINGTON, D.C. 20544

March 25, 1986

Honorable Peter W. Rodino
Chairman, Committee on the Judiciary
U.S. House of Representatives
2137 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

This is in further response to your request for the views of the Judicial Conference on H.R. 3378, the Electronic Communication Privacy Act of 1985. At the meeting of the Judicial Conference on March 12-13, 1986, the Conference considered H.R. 3378. After reviewing provisions of the bill, the Conference recommends to Congress that, if legislation is enacted to require prior judicial authorization for the use of pen registers and tracking devices, the legislative history should note that a judge has the authority to designate a magistrate to entertain applications and issue orders approving the installation and use of a pen register or tracking device.

If we may be of any further assistance to you with respect to this issue, please contact Christy Massie at 633-6040 in the Legislative Affairs Office.

Sincerely,

L Ralph Mecham

L. Ralph Mecham
Director

cc: Honorable Hamilton Fish, Jr.
Honorable Robert W. Kastenmeier
Honorable Carlos J. Moorhead

**RADIO-TELEVISION NEWS DIRECTORS ASSOCIATION**

RTNDA

EXECUTIVE VICE PRESIDENT
Ernie Schultz
1735 DeSales Street, N.W.
Washington, DC 20036
(202) 737-8657

PRESIDENT
John Spain, WBRZ-TV
Baton Rouge, LA

PRESIDENT-ELECT
J. Spencer Kinard, KSL-TV
Salt Lake City, UT

TREASURER
Lou Prato, Medill News Service
Washington, DC

PAST PRESIDENT
Lou Adler, WOR Radio
New York, NY

REGIONAL DIRECTORS
Bill Ewing, KPTV
Portland, OR (1)
Carole Cooper, KUTE/KGFJ
Los Angeles, CA (2)
Hal Kennedy, KKTV
Colorado Springs, CO (3)
Bill Goodman, KPRC-TV
Houston, TX (4)
Tom Bier, WISC-TV
Madison, WI (5)
Bob Priddy, Missouri Network
Jefferson City, MO (6)
Dave Ellsworth, WGN Radio
Chicago, IL (7)
Bob Brunner, WSAZ-TV
Huntington-Charleston, WV (8)
Stuart Kellogg, WWL-TV
New Orleans, LA (9)
Chris Schmich, WREG-TV
Memphis, TN (10)
Jeff Marks, WCSH-TV
Portland, ME (11)
Rob Sunde, ABC Radio
New York, NY (12)
Harvey Powers, WWBT-TV
Richmond, VA (13)
Tom Wayne, WTOG-TV
St. Petersburg, FL (14)
John Hinnen, CFTR Radio
Toronto, Ontario, Canada

DIRECTORS-AT-LARGE
Tom Becherer, WLKY-TV
Louisville, KY
David Lampel, WBLS/WLIB
New York, NY
Mary C. McCarthy, WYFF-TV
Greenville, SC
Steve Vogel, WJBC/WBNQ
Bloomington, IL

EX-OFFICIO
Dick Gage
President, NBEA
WHBF AM/FM/TV
Rock Island, IL
Sarah Toughes
Chair, AEJMC Radio/TV Division
University of Illinois
Champaign, IL

PRESIDENT, RTNDA CANADA
Ian Stanley
Canadian Broadcasting Corp.
Toronto, Ontario, Canada

March 18, 1986

HAND DELIVERY

The Honorable Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties
and the Administration of Justice
Committee on the Judiciary
United States House of Representatives
2328 Rayburn House Office Building
Washington, D.C. 20575

Dear Chairman Kastenmeier:

The Radio-Television News Directors Association (RTNDA) submits the following views regarding certain provisions of H.R. 3378, the "Electronic Communications Privacy Act of 1985," that are of particular concern to those involved in the gathering and dissemination of news.

RTNDA is a professional organization of more than 2,000 new directors and others who are active in the supervising, reporting and editing of news and public affairs programming on radio and television, both broadcast and cable.

The provisions of H.R. 3378, specifically Section 101(b) of the bill, appear designed to preserve what is today the standard newsroom practice of monitoring various public safety and related governmental communications systems. RTNDA strongly supports the Chairman's stated intention to maintain media access to these important sources of information. In certain respects, however, the existing language of Section 101(b) does not effectuate this intent.

BEST COPY AVAILABLE

First, in Section 101(b), which would amend 18 U.S.C. § 2511 to create a new subsection (g), the language of subsection (g)(ii)(I) should be revised to reflect the intent of Section 705(a) of the Communications Act, 47 U.S.C. § 705(a). Section 705(a) permits the interception of, among other things, radio communications which are transmitted by any station for the use of the general public or which relate to ships, aircraft, vehicles, or persons in distress. Corresponding language has been included in subsection (g)(ii)(I) of the bill, but the latter eliminates the disjunctive separation between the exemptions, thereby qualifying the phrase "transmission by any station for the use of the general public" -- in other words, traditional broadcasting -- with the phrase "which relates to ships, aircraft ..." etc. In order to make clear the Subcommittee's intent to preserve long-recognized and independent exemptions for the interception of 1) publicly broadcast communications and 2) those which relate to persons or vehicles in distress, subsection (g)(ii)(I) should be amended to provide that it shall not be unlawful under this chapter for any person to intercept any communication transmitted

> by any station for the use of the general public, or which relates to ships, aircraft, vehicles or persons in distress; (underlined word added).

Second, the language of subsection (g)(ii)(II) is not broad enough to preserve current newsroom practice in monitoring not only police and fire transmissions, but a range of other public safety and related communications systems that are "readily accessible to the general public." At present, it is standard practice for news personnel to scan a variety of communications frequencies that carry information concerning activities of potential general public interest and about which there is no expectation that the communications will not be overheard. While police and fire transmissions are the most obvious sources of such information, news organizations also monitor frequencies employed, for example, by other federal, state and county law enforcement agencies, civil defense organizations, or FAA airport personnel. In areas near harbors and coastal regions, newsrooms may also monitor a variety of ship-to-shore communications (e.g., Coast Guard frequencies) and, in severe weather conditions, the media may scan frequencies employed by various branches of the National Weather Service.

It is evident that, in all such instances, the transmissions are not encrypted and the governmental and other authorities involved are aware that news organizations, as well as the general public, have access to these communications. The practice of monitoring these frequencies thus raises no privacy or other concern. This conclusion is reinforced by the fact that, consistent with accepted practice, the media do not publicly re-broadcast any such monitored communications, but utilize the information simply to alert their news staffs to a possible event of public interest, which is then investigated by reporters dispatched to the scene for the purpose of confirming the truth and accuracy of an initial police, traffic, or air controller report.

The language of proposed subsection (g)(ii)(II) should therefore be amended so as to create an exemption for the interception of any communication transmitted

> by a walkie talkie or by any marine, aeronautical, law enforcement, civil defense, governmental or public safety communications system, including a police or fire communication system, that is readily accessible to the public.

With the inclusion of this and the other change specified above, we believe that the public's access to these important sources of news reporting can be preserved. RTNDA very much appreciates the Chairman's expressed sensitivity to this issue and looks forward to working with the Subcommittee so as to effectuate this intent.

Sincerely,

John Spain

John Spain
President

JS:dhr

cc: Members of the Subcommittee on Courts,
Civil Liberties and the Administration
of Justice

[illegible]

**The Chase Manhattan Bank, N.A.**
1 Chase Manhattan Plaza
New York, New York 10081

**F. W. Gerbracht, Jr.**
Vice President

CHASE

March 17, 1986

The Honorable Robert W. Kastenmeier
House Office Building
Washington, D.C. 20415

Dear Congressman Kastenmeier:

Your subcommittee is considering landmark legislation that will revise our nation's privacy laws to reflect the enormous changes wrought by the revolution in information technology. The Electronic Communications Privacy Act of 1986, H.R. 3378 and S. 1667, would update traditional law protecting the privacy of telephone calls and letter mail, in order to protect the privacy of modern forms of communication.

Technological revolution in telecommunications and computing has transformed radically the ways in which individuals and businesses communicate. Yet these new forms of communications are left exposed to interception and intrusion by unauthorized individuals and by government authorities without sufficient authorization, because of gaps created in privacy law by technological progress. These gaps create anomalous situations in everyday life, ones that demand legislative remedy:

- o Transmission of personal or business data to and from a computer are unprotected from unauthorized interception and intrusion, while personal or business voice transmissions are protected. As bankers, we are particularly concerned about the confidentiality of customer financial transactions being received and delivered electronically.
- o Electronic mail when in transmission and when stored in an addressee's electronic mailbox is unprotected, while U.S. postal mail is protected.
- o Electronic transmissions of information when stored in communications or computer systems are unprotected.
- o Cellular radio telephone calls from a car are unprotected, while calls from the home or office normally are protected.

The Electronic Communications Privacy Act will extend essential privacy protections to the communications of today and tomorrow. In so doing, the Act will:

- o protect the privacy of personal and corporate communications regardless of the technology used.
- o enhance the public's acceptance and use of new information technology in their daily lives and business operations.
- o ensure the burgeoning growth of the information and service industries that are strategically critical to this nation's productivity and to the obtainment of national goals.
- o ensure the continued viability and growth of the electronic mail, electronic funds transfer, computer services, videotex, database and telecommunications industries.

For these reasons, the Chase Manhattan Bank, N.A. supports the Electronic Communications Privacy Act of 1986 in principle.

Sincerely yours,

F.W. Gerbracht, Jr.,
Director of Data Security

copy: Chase Congressional Liaison Office

BEST COPY AVAILABLE

MAR 21 1986

ACLU
WASHINGTON OFFICE

122 Maryland Avenue, N
Washington, DC 20002
(202) 544-1681

National Headquarters
132 West 43rd Street
New York, NY 10036
(212) 944-9800

Norman Dorsen
PRESIDENT

Ira Glasser
EXECUTIVE DIRECTOR

Eleanor Holmes Norton
CHAIR
NATIONAL ADVISORY COUNCIL

March 14. 1986

Hon. Robert Kastenmeier
House Judiciary Committee
2328 RHOB
Washington, DC 20515

Dear Rep. Kastenmeier:

On behalf of the American Civil Liberties Union, I am writing to express our strong support for H.R. 3378, the Electronic Communications Privacy Act of 1986 introduced by Rep. Carlos Moorhead and you last year. The principal aim of H.R. 3378 is to update federal law to extend privacy protection to new forms of communications. This landmark legislation is of the utmost importance and needs to be enacted into law. We commend your efforts.

Over the last decade new technologies have brought about fundamental changes in the ways citizens and businesses communicate private messages. New forms of computer driven "data" communications such as electronic mail services are augmenting or taking the place of telephonic voice communications and traditional mail sent through the postal system. Wire, microwave, cellular radio and other transmission means are carrying voice, text, and video messages and images separately and in combination. Such messages are being carried not only by common carriers but by new private communications entities.

The need for legislation arises from the now widely held view that federal law has not kept pace with communications innovations and affords little if any legal protection against unauthorized government or private interception of new forms of communication. The principal statute, Title III of the Crime Control and Safestreets Act of 1968, only prohibits unauthorized government or private interception of voice communications carried in part by wire over common carrier systems. In the face of the current communications revolution, this law is simply out of date.

H.R. 3378 would amend Title III to prohibit the unauthorized interception of private data and voice communications regardless of the technical means of communication. It would establish in law the fundamental privacy principle that the "contents" of a private message should be protected regardless of its form or means of communication. As a matter of law, it should not make a difference whether a person communicates with another party by having a phone conversation or sends the same message in text over a phone line using a computer, a modem, and an electronic mail service. Nor should it make a difference whether a communication is carried by wire, microwave, or cellular phone service.

H.R. 3378 would also establish essential privacy protection for certain electronic records generated by new forms of communication. It recognizes that privacy protection would be illusory if the statute only barred unathorized interception of messages while being communicated without also barring unauthorized private or unwarranted government access to electronically stored messages and data created by new communications technologies. For this reason, the statute would require the government to obtain a search warrant to obtain electronic messages temporarily stored by electronic mail companies either for forwarding to addressees or for system integrity and security. The statute also protects the privacy of customer records and data electronically communicated and stored with entities providing remote computing services.

H.R. 3378 is comprehensive legislation designed to establish a rational overall protection scheme for private communications. Such an approach is essential. The heretofore piecemeal approach to the problem of communications privacy has created significant legal uncertainty. Because Title III is technology specific, new means of communication have no statutory privacy protection. While we believe messages communicated by new technologies are protected under the Fourth Amendment, communications privacy law unfortunately has not evolved into a coherent set of legal precedents. Because legal uncertainty threatens privacy rights as well as the viability and growth of new communications industries, Congress should enact this legislation. As you know, a broad coalition of business, computer, and communications firms support H.R. 3378.

H.R. 3378 would also clarify the warrant requirements of Title III and establish minimum safeguards for the investigatory use of new electronic surveillance techniques such as pen registers and tracking devices. We strongly endorse these provisions and urge their adoption.

In conclusion, we urge support for H.R. 3378 and will work for its enactment. We are anxious to work with you on this legislation.

Sincerely,

Jerry J. Berman
Chief Legislative Counsel

ASSOCIATION
OF AMERICAN
RAILROADS

William H. Dempsey
President

March 14, 1986

The Honorable Robert W. Kastenmeier
Chairman, Subcommittee on Courts, Civil
  Liberties and the Administration of
  Justice
Committee on the Judiciary
United States House of Representatives
House of Representatives Rayburn Office
  Building-Room 2328
Washington, DC 20515

Re: H.R.3378--The Electronic
Communications and Privacy
Act of 1985

Dear Mr. Kastenmeier:

The Association of American Railroads (AAR), on behalf of the Railroad Industry of the United States, has been considering the above referenced proposed legislation. While having concern as to some of the specifics as advanced below in this letter, the AAR does support the broad aim of H.R. 3378 toward providing the legal protections of privacy and security which the new telecommunications and computer technologies need to better serve all of the American public.

Noting the foregoing, the railroads are interested in H.R. 3378 because the industry depends heavily upon telephone, mobile radio, and point-to-point microwave communications for the conduct of its operations in providing safe and reliable transportation service to the American public. Additionally the industry is a major user of computers and the telecommunications required to move large amounts of data to, from, and between computers. AAR's concern is that the proposed legislation, while striving to provide privacy, has a consequential effect in these communications areas that, unless clarified, could impair important railroad operations.

50 F Street, N.W., Washington, D.C. 20001 (202) 639-2402

As read by AAR, H.R. 3378 would bar intercept of electronic communications (both wire and radio), unless there is a specific exception. Section 101(b) of S.1667 sets forth "Exceptions with Respect to Electronic Communications" and one of the provisions, specifically (g)(i), provides it shall not be unlawful "to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public." The AAR's concern with this exception as currently drafted extends to the broad scope of "electronic communications" which would be included and to the possible interpretation of the phrase "readily accessible to the public." If the latter phrase were interpreted in an unrestrictive manner, then the exception would expose radio transmissions passing over microwave circuits to interception beyond the reach of the federal law. Conversely, if the phrase "readily accessible to the public" were interpreted in a restrictive manner, the use of land mobile radio communications would be severely restricted.

The railroad industry operates approximately 44,000 route miles of microwave communications. Large volumes of data and computer-to-computer traffic are exchanged over the industry's microwave communications systems. Most of this information is priviliged and clearly it should not be "legal" for unauthorized parties to intercept such traffic. Yet, if the microwave circuits were deemed to be "readily accessible to the public", they would fall within the exception.

Land mobile radio communications have become essential to the safe and efficient operations of the nation's railroad systems. While there are many applications of land mobile radio in the railroad industry, probably the most important are those used by railroad dispatchers, yardmasters, and terminal supervisors. It is essential for the latter personnel to have a complete and accurate picture of "what is going on" in their areas of supervision. Involved is extensive monitoring of and listening to over-the-air land mobile radio transmissions. Specifically main line train dispatchers listen to transmissions from locomotives, particularly in end-to-end connections so that they remain aware of what is happening in their dispatch territory. Railroad yardmasters constantly monitor radio transmissions to keep abreast of operations and events within the yards for which they are responsible. Similarly, terminal supervisors constantly monitor to keep abreast of movements within a train terminal. As a final point, train crews monitor the transmissions of other train crews to stay informed of operational activities. The point is that intercepting and monitoring of railroad land radio traffic by the railroad industry's own personnel is an essential part of safe and efficient operations.

However, if the phrase "readily accessible to the public" were interpreted in a manner restrictive enough to exclude radio microwave communication from the exception, there is a possibility that interception of mobile radio communication would also be illegal under the terms of H.R. 3378 as presently written.

Furthermore, radio frequencies licensed by the Federal Communications Commission for railroad usage are shared by more than one railroad licensee. Some railroad frequencies are shared with non-railroad users as well. The result is that "inadvertent interception" could occur frequently from either the shared frequency usage or from checking to assure that a frequency is clear prior to commencing a transmission. AAR would point out those practical radio procedures should not be made illegal in the course of enacting legislation for privacy in electronic communications.

Importantly, it is not necessary that the language of the exception be so broad as to cover all "electronic communications." It is only necessary that the exception extend to mobile radio communications. If that were accomplished, it would then be unnecessary to add the limiting reference to "readily accessible to the public." In order to meet this objective, AAR suggests Section 101(b) of H.R. 3378 be modified so that the proposed new paragraph (g)(i) would read:

"(g) It shall not be unlawful under this chapter for any person--

"(i) to intercept, use, or disclose a non-communication common carrier mobile radio transmission".

The foregoing proposed change would remove operational-fixed microwave circuitry from the "exceptions" and place the focus of the exception on to the mobile radio operations of users who are not communications common carriers.

For information, since S. 1667 contains parallel text to H.R. 3378, the above letter is also being sent to Senator Charles McC. Mathis, Chairman Subcommittee on Patents, Copyrights & Trademarks, Committee of the Judiciary and Senator Patrick J. Leahy.

Sincerely,

W. H. Dempsey

STATEMENT OF

EDWARD O. FRITTS
PRESIDENT,
NATIONAL ASSOCIATION OF BROADCASTERS

BEFORE THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTIVES

CONCERNING

H.R. 3378
ELECTRONIC COMMUNICATIONS PRIVACY ACT

March 7, 1986

nab

# STATEMENT OF
# EDWARD O. FRITTS
# PRESIDENT
# NATIONAL ASSOCIATION OF BROADCASTERS

Mr. Chairman, members of the Subcommittee. My name is Edward O. Fritts. I am President of the National Association of Broadcasters ("NAB").[1] I am pleased to have the opportunity to present this statement for the record on H.R. 3378, the Electronic Communication Privacy Act.

The introduction of H.R. 3378 marked an important turning point in our national recognition of the impact of technological change upon the privacy of communications. As Chairman Kastenmeier noted in his floor statement upon this bill's introduction, the "new modes of communication have outstripped the legal protection provided under statutory definitions bound by old technologies."

The innovative technologies for private data and voice transmission being introduced by America's broadcasters are an integral part of the information transmission revolution. NAB believes the proposals made in H.R. 3378 will, if adopted, make an important contribution to the assurance of confidentiality, and thus the future success of these transmission technologies. We strongly support these proposals. We do find, however, that some modifications should be made in the bill in order to assure the legality of the continued monitoring of certain readily available radio transmissions by the news media. While the Chairman's floor statement envinces an intent to allow receipt of these communications to continue unimpeded, the language of the bill requires some broadening to achieve the desired result.

---

[1] NAB is a nonprofit incorporated association of radio and television broadcast stations and networks. NAB membership includes more than 4,500 radio stations, 890 television stations and the major commercial broadcast networks.

Permit me to first address the private transmission services now being offered by or utilizing the facilities of broadcast stations. The broadcast band allocated to a particular station allows for the transmission of more "information" than the regular over-the-air broadcast signal with which we are all familiar. Some of this spectrum is frequently designated for use to fill the station's own internal needs. However, many other uses are possible. Until relatively recently, these alternative uses were precluded by FCC rules -- with the best known permitted alternative being the transmission of "background music" over the subcarrier channels, or "SCAs," of many FM radio stations.

Over the past few years, however, the FCC has lifted most of the limitations on the types of information a broadcaster can transmit over that part of the spectrum allocated to his station but not susceptible to listening or viewing by the general public. The result has been an explosion in the variety of data transmitted by broadcasters for the use of a limited private audience.

This is particularly the case in FM radio. Present and planned uses of FM subcarrier frequencies include transmission of paging signals, electronic mail, computer software, and a variety of text and data for business applications. Similar data transmission on the "vertical blanking interval" of the television signal is emerging. The capability for data transmission by AM radio is more limited. However, a key new use for AM is utility load management. It is important that the private information transmissions users expect to be private do in fact have such protection at law.

Clearly, the intent of H.R. 3378 as drafted is to provide coverage of such transmissions. NAB is opposed to any attempt to reduce the scope of this legislation either by eliminating from its purview certain types of transmissions, such as paging, or by requiring encryption as a precursor to protection. While in some situations transmissions will be encrypted or "scrambled," it is in any case a fact that the transmissions in question are not intended for or readily accessible to the general public. Special receivers are necessary. Further, in most circumstances, those turning to these frequencies when they are being used for paging or data transmission would, absent additional special equipment, receive an unintelligible electronic sound, even without encryption.[2] We urge the Subcommittee to maintain the original intent of this legislation as it moves to markup.

---

[2] This is not, of course, the situation if a subcarrier is being used for unencrypted voice transmission such as a radio reading service for the blind.

In one area of special concern to the media, the Subcommittee's purpose is clear, but some additional redrafting appears necessary to effectuate the Subcommittee's intent. That is the area of public safety and related communications that are regularly monitored by newsroom personnel.

Although we know from the Chairman's statements that the Subcommittee does not intend to cut off access to these important sources of information, the exemptions now in the bill do not clearly maintain that access.

We have several suggesstions which, although perhaps not the last word on this subject, may serve to alleviate this problem. First, we believe that in section 101(b) of the bill, which amends 18 U.S.C. § 2511 to create a new subsection (g), proposed subsection (g)(ii)(I) should be reworded to reflect the present intent of section 705(a) of the Communications Act, so that the subsection (g)(ii)(I) would read -- "(I) by any station for the use of the general public, or which relates to ships, aircraft, vehicles or persons in distress;" (underlined word added).

This phrasing makes clear that the exemption for communications for the use of the general public -- that is, traditional broadcasting -- is separate from the exemption for communications about people or transport vehicles in distress.

Secondly, we would amend proposed subsection (g)(ii)(II) to read --

"(g)(ii)(II) by any marine radio system, aeronautical radio system, governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the public;"

We would couple this statutory subsection with strong report language making clear that this subsection is to be given a very broad reading. Allow me to explain our reasoning in asking for these changes.

It is, and has been for many years, standard newsroom practice to regularly monitor a variety of newsworthy communications frequencies, as to which we truly believe there is no reasonable expectation of privacy. While police and fire are the prime examples, the potential range is much broader. In port and water-related communities, there is likely to be some monitoring of Coast Guard and ship-to-shore transmissions, while in areas near airports, the air-to-ground frequencies are often scanned. It is no secret that news people, like the communications hobbyists who have testified before the Subcommittee, have been monitoring these frequencies for many years. A report heard on the scanner radio is not, of course, then put out over the air or into print by the broadcaster or newspaper. Rather, it serves as the information source basis on which reporters are assigned, calls made, and a story assembled for the public.

Reporting of this news is an important public service of the broadcast and print media. Those transmitting on these frequencies are well aware that this monitoring is occurring. It is information which the people have come to expect, and deserve to have. We know that the Subcommittee does not want to present obstacles to these journalistic practices, and look forward to working with you to refine the language of the bill to that end.

Finally, I wish to briefly address H.R. 3378's treatment of broadcast network satellite feeds, as to which issue has been raised by the January 30, 1986, statement of Richard L. Brown, general counsel of the Satellite Television Industry Association, Inc./SPACE, and Mr. Brown's accompanying letter to Chairman Kastenmeier, dated January 28, 1986.

In the Cable Communications Policy Act of 1984, Congress amended section 605 of the Communications Act to create a limited exemption from that section's restrictions on unauthorized reception and use of radio transmissions for home viewing of unscrambled satellite cable programming.[3/] The exemption only applies if no marketing system for such programming has been established. No statutory "safe harbor" was created for encrypted ("scrambled") satellite cable programming.

For the purpose of the special exemption, satellite cable programming was defined as "video programming which is transmitted via satellite and is primarily intended for the direct receipt by cable operators for their retansmission to

---

[3/] The Cable Communications Policy Act also numbered the previous § 605 as § 705(a). The limited exemption was included in new § 705(b).

cable subscribers."[4] Clearly, this definition does not include broadcast network satellite feeds, which are intended for receipt only by a network's local station affiliates.

Section 101(b) of H.R. 3378 recognizes the limited satellite cable programming exemption by stating that

> It shall not be unlawful under this chapter for any person . . . to engage in any conduct which . . . is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act.

In his January 30, 1986, submission, Mr. Brown has made a somewhat disingenuous proposal for modification of the existing H.R. 3378 text, contending that the bill as presently drafted might be "misconstrued" to prohibit activity which is not barred by section 705(a). The language proposed by Mr. Brown appears intended to create a presumption that reception of satellite-distributed programming not otherwise exempted from section 705(a) is nonetheless legal. However, I believe that the information submitted to the Subcommittee by the FCC's General Counsel and by the law firm of Wiley & Rein, counsel for CBS Inc., clearly indicates that the contrary is the case.[5]

---

[4] Emphasis supplied. The definition is found in new § 705(c)(1).

[5] Letter to Chairman Kastenmeier from FCC General Counsel Jack D. Smith, dated November 27, 1985; letter to Chairman Kastenmeier from Robert A. McConnell, Vice President, CBS Washington, with appended Wiley & Rein memorandum, dated February 4, 1986. While we do not agree with the conclusions drawn in Mr. Brown's statement and letter, they are consistent with the legal theory he has developed to justify the otherwise unauthorized interception and disclosure or use of satellite signals by dish owners. See Brown & Helland, Section 605 of the Communications Act: Teaching a Salty Old Sea Dog New Tricks, 34 Cath. U.L. Rev. 635 (1985).

I wish to associate NAB with those analyses, which I see no need to reiterate here.[6]

The treatment of broadcast network satellite feeds as private is consistent with Chairman Kastenmeier's view that new tecnological means of information transmission be given the same protection afforded to conventional communications. As I observed in my December 13, 1985, letter on "scrambling" to all members of the Judiciary Committees of both the House and the Senate, networks have until recently used land lines similar to long distance telephone lines to supply programming to local stations for broadcast. Telephone lines have also been used to "back haul" feeds of news and sports events from their origination points to network control centers.

The advent of low cost, reliable satellite television systems has led to the increasing use of that technology for program distribution to both radio and television stations. While, in television, the three major commercial networks and PBS are the leading users of satellite transmissions, the technology is increasingly also being utilized by the new programming networks and program distributors serving independent stations.

---

[6] It is useful to note the unequivocal statement of Chairman Wirth of the House Telecommunications Subcommittee on this issue. In a letter to the New York Times discussing the meaning of the Cable Act's satellite cable section, Chairman Wirth commented that "the law continues to prohibit any unauthorized use of noncable-television satellite signals . . . ." Wirth, No Free Lunch in the New Satellite-Dish Law, N.Y. Times, December 18, 1984, at A-30.

No one has ever questioned the privacy protection afforded program feeds transmitted by telephone wire, and there is no apparent reason why this protection should not be continued when the same material is distributed by satellite. Although the broadcast programming in question is in some instances being scrambled, current law does not nor should it require encryption as a precondition of protection.

The broadcast-related satellite television feeds in dispute were never intended to be delivered directly to viewers' homes. They do not contain the local business and political advertising, public service announcements, and news and weather bulletins inserted by local stations. They do not, of course, include any locally produced news and public affairs programming. They do include private network-to-station scheduling information, program previews, material related to the business operations of the networks and affiliates, and raw program materials intended for insertion in local news and sports programming. Diversion of audiences to these feeds through the unauthorized receipt of satellite transmissions reduces the audience ratings of the local network affiliates, and, thus, the dollars paid for ads, undermining the financial stability of our free, over-the-air system of broadcasting.

Mr. Brown paints a picture of a wonderful world of programming abundance available to satellite dish owners. We in the broadcasting industry do not believe that the source of this abundance should include the private satellite programming transmissions intended for the nation's over-the-air broadcast stations. We commend the Subcommittee for the approach it has taken to this issue in H.R. 3378, and strongly oppose any change in the relevant language of Section 101(b) currently included in the bill.

While taking this position, we are not insensitive to the desires of the roughly one million households located in rural areas which do not receive over-the-air television. We believe that after those who nonetheless receive or could receive broadcast signals through the cable systems in their areas are taken into account, only about half of the households in question lack access to broadcast station signals.

Perhaps the best way to solve this problem is by the extension of broadcast service through "translator" stations. Translators expand the reach of over-the-air stations through rebroadcast. Unfortunately, the FCC has lumped translator applications in with low power TV applications. Thus, translator applications must compete for frequency allocations in the low power lotteries. So long as this situation continues, it is impossible for any planned expansion of translator service to be put in place. Congressional assistance in resolving this problem would be welcomed.

In closing, I would like again to thank the Chairman and the members of this Subcommittee for the important action being taken in communication privacy with this legislation, and for your consideration of the modifications we have requested.

**ASSOCIATION OF NORTH AMERICAN RADIO CLUBS**

Richard T. Colgan, Executive Secretary
Post Office Box 180403
Austin, Texas 78718-0403
U.S.A.
Phone (512) 451-5897

SUPPLEMENTAL STATEMENT

CONCERNING

H.R. 3378

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985

FEBRUARY 27, 1986

## INTRODUCTION

This document introduces additional information from the Association of North American Radio Clubs (ANARC) for consideration by the House Committee on the Judiciary's Subcommittee on Courts, Civil Liberties and the Administration of Justice.

In the Association's January 30, 1986 written statement and oral testimony before the Subcommittee, we did not focus on the particular question of cellular radiotelephony because the wording of H.R. 3378 is so much broader. We have now seen how much attention the Subcommittee is paying to the perceived needs of that one industry, and how seriously the industry has misrepresented its situation. While we have no animosity towards cellular, we cannot sit idly by while they use their influence to make dubious changes in public policy, largely to benefit their bottom lines, while denying what is clearly their responsibility.

Consequently, much of this document is devoted to supplying information about cellular radiotelephones which we believe the Subcommittee needs to know if it is to produce a revised version of H.R. 3378 which accurately reflects the facts.

Throughout this statement the terms "cellular radiotelephone", "cellular phone", "cellular telephone" and "cellular" are used interchangeably.

This document and our January 30 written statement and oral testimony before the Subcommittee, represent the position of the Association of North American Radio Clubs on H.R. 3378, the Electronic Communications Privacy Act of 1985.

## RECOMMENDED AMENDMENTS TO H.R. 3378

The Association reaffirms its commitment to the four amendments to H.R. 3378 proposed in our statement and oral testimony on January 30. Those amendments, as well as the two which follow in this document, are listed and briefly explained in Attachment 1. If incorporated in the bill, we believe these six amendments will substantially reduce our concerns about the potentially devastating impacts of this legislation on the millions of average Americans who own and enjoy shortwave radios and scanners.

Definition of "Electronic Communication"

Since presenting our testimony, we have read and studied the November 13, 1985 statement submitted to the Senate Committee on the Judiciary, Subcommittee on Patents, Copyrights and Trademarks, by Dr. Lynn W. Ellis (Chairman of the IEEE's Committee on Communications and Information Policy). Dr. Ellis makes a number of extremely insightful comments and suggestions, and we urge that these recommendations be considered as changes to H.R. 3378 are discussed. For convenience, we have attached (as Attachment 2) the section of his testimony entitled "Proposed Changes in Wording of S. 1667 and Reasons for Changing".

In general, ANARC supports most of the proposed changes offered by Dr. Ellis. In particular, we draw attention to the one described in his section 1.d., in which he proposes the addition of the BOLDFACE (underlined in the original) phrase to the definition of "electronic communication":

> "'electronic communication' means any...transmission of signs, signals, writing, images, sounds, data or intelligence of any nature...by wire, radio, electromagnetic or...[photoelectronic] system that affects interstate or foreign commerce WHERE THE PERSON ORIGINATING SUCH COMMUNICATION EXHIBITS AN EXPECTATION THAT SUCH COMMUNICATION IS NOT SUBJECT TO INTERCEPTION UNDER CONDITIONS JUSTIFYING SUCH EXPECTATIONS."

The BOLDFACE phrase is a slight paraphrasing of the language presently found in Section 2510(2) of Title 18 of the United States Code, in the definition of "oral communication". This language seems to have been inserted in the Code in recognition that those communicating by wire, where the communication can be sent safely to its intended recipient, and those communicating orally by inherently less secure modes, may not have the same expectations of privacy. In the case of WIRELESS oral communications, expectations are not by themselves sufficient to establish a Federally-protected right of privacy: the "conditions justifying such expectations" must also be present.

Dr. Ellis points out that it is inconsistent to preserve a "reasonableness test" for expectations of privacy in "oral communication" while omitting one for "electronic communication", as does the current draft of H.R. 3378. We could not agree more strongly. And we concur with Dr. Ellis when he states that if a reasonableness test is to be excluded from the definition of "electronic communication", "...it is critical that the legislative history provide some rationale as to why...electronic communications are to have absolute protection...."

Reexamining H.R. 3378 in light of his suggestion, we can see how the lack of a reasonableness test creates many of the problems we noted in our January 30 testimony. The present, overly-broad definition of "electronic communication" would confer a Federally-protected right on systems that have neither the need nor the expectation of privacy, as well as on systems that have not themselves taken even minimal precautions against casual interception. Extending a near-absolute right of privacy to electronic communications without regard to the circumstances of the communication borders on the ridiculous.

Definition of "Intercept"

In his written statement submitted to the Subcommittee on Courts, Civil Liberties and the Administration of Justice on January 30, 1986, Mr. Neal J. Amick of AT&T proposed an amendment to H.R. 3378 that would greatly enlarge the definition of the word "intercept". The following is quoted from page four of his statement:

> "The H.R. 3378 definition is ambiguous because it involves the definition of a term with a derivation of the same term. It reads:
>
> > "intercept" means the interception of the contents of any electronic or oral communication through the use of any electronic, mechanical or other device.
>
> We recommend that the word "interception" be replaced with a series of words that would include, as a minimum: acquisition, reception, recording and copying. We also recommend that the word "contents" be deleted.... Finally we recommend that the definition of "intercept" be reworded to include the interception of any portion of a communication."

The effect of this proposal, if passed into law, would be to make the mere RECEPTION of an electronic or oral communication unlawful; not just the content, but even the electromagnetic radiation carrying it. This is absurd!

There are situations where reception of some signals is practically unavoidable. Such situations occur throughout the country every day. The most common situation is a phenomenon known as intermodulation. "Intermod" is the result of FM signals transmitted by different stations on different frequencies "mixing" in a receiver so that both signals can be heard on frequencies on which neither is actually transmitting.

The most common example of intermod in the Washington, DC area occurs when the fire department and the Veterans Administration hospital paging system are on the air simultaneously. Both their transmissions can be heard on dozens of frequencies scattered across the VHF radio band. Many combinations of transmissions cause intermod; it is almost endemic to FM. Making mere reception of such signals illegal would make it hard to use FM receivers in populated areas without the receiver owners unintentionally engaging in criminal activity.

The Subcommittee may know that last year the Federal Communications Commission set national guidelines to limit human exposure to radio emissions (Attachment 3). The U.S. Environmental Protection Agency is also considering action in this area, and some state and local governments have recently passed laws establishing local standards. These are responses to the growing evidence that exposure to even low levels of non-ionizing radiation can produce biological effects that are not well understood. AT&T's proposal would make it unlawful to determine compliance with any exposure standards.

These are practical problems. The AT&T proposal is also acutely problematic in principle. To understand why, consider that visible light and radio are the same "substance"; it is more than a metaphor to say that radio frequencies are "colors" that the eye cannot see but that radios can. Translating the AT&T proposal into its visual analog clarifies the issue considerably. If someone in Times Square holds up a large sign saying "Irma, I Love You," it will be seen by many thousands for whom the message is not intended. The person holding the sign may want only Irma to see it. Taking a cue from AT&T, he might ask Congress to make it unlawful for anyone but Irma to read the message! Would the Congress take him seriously?

It is the nature of radio that by extending communications beyond the range of human eyes and ears, the communicator's signals, perhaps unknown to him, penetrate the homes and personal spaces of many more people than just his desired recipient. AT&T's proposal is stunning in its arrogance; it asserts the right to electronically invade anyone's space, while denying him or her the right to detect the invasion.

If the AT&T language were to be incorporated in H.R. 3378, we would consider attempting to have a bill introduced that would make it unlawful to transmit private electronic communications into any space other than that occupied by the intended recipient of that communication. The logic and the benefit to privacy would be the equivalent of AT&T's offering.

Electromagnetic radiation, whether it is ambient light or radio waves, is NOT private property. Those who are licensed to use a particular frequency for a particular purpose do not own the frequency. We regard the AT&T proposal as an attempt to establish OWNERSHIP RIGHTS in the radio spectrum, using the privacy issue as a pretext. This attempt to privatize an aspect of the PUBLIC DOMAIN goes far beyond the rights now granted to licensees by the Federal Government.

We believe that the definition of "intercept" in the current version of H.R. 3378--referring to the acquisition of the content of a communication--correctly draws the line between that part of the communication that may be entitled to privacy protection and the part which--in the case of radio transmission--is a PUBLIC DOMAIN resource. In the case cited by AT&T to justify omission of the word "content" from the definition--one individual receiving a communication without extracting its contents and then passing it on to another for decryption--by treating the two individuals as "partners in crime", would not the result of their joint action be prosecutable as an interception of content?

As for the ambiguity of using "interception" as part of the definition of "intercept", the problem can easily be avoided by returning to the word--acquisition--used in the definition in Section 2510(4), Title 18 of the United States Code. Simply deleting the word "aural" from the existing definition in the Code would seem to accomplish the purpose sought in H.R. 3378:

> "'intercept' means the acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."

COMMENTS ON EXEMPTIONS FROM PROHIBITION ON INTERCEPTION UNDER H.R. 3378

The present draft of H.R. 3378 attempts to overcome the excessive sweep of the term "electronic communication" by including, on page three, a list of specific types of communication which would be excluded from the privacy protection offered in the bill. During the

January 30 Subcommittee hearing on the bill, Mr. Kastenmeier remarked:

> "We may not have anticipated all the exclusions, nor have drawn it up, from a policy standpoint, as precisely as we need to, or would wish."

Similarly, a member of the Subcommittee staff suggested to us that we might resolve our concerns about the bill by submitting a list of communications that we felt should be excluded.

After further discussion on this point, we have concluded that trying to correct a too-broadly worded general rule by proposing specific exceptions is not the best way to proceed. Changes in technology are soon likely to make any such list obsolete. In Mr. Kastenmeier's statement to the Senate Subcommittee on Patents, Copyrights and Trademarks on November 13, 1985, he noted:

> "Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today...is destined to be outmoded within a few years."

Exactly the same can be said of any attempt to write a law which exempts from protection only specific current technologies and services.

For example, "walkie-talkies" would be exempted by the present bill, even though many radio services that now require bulkier equipment are likely to use "walkie-talkies" in the near future. Some units with encryption capabilities are already on the market. Should the latter be denied protection, when the user's expectation of privacy is both evident and reasonable?

We submit that compiling a definitive list of exclusions would pit service against service, the manufacturers of one class of equipment against the manufacturers of other classes. The process would be time-consuming and controversial, without yielding a list likely to be valid five years from now.

We are not proposing that H.R. 3378 should not contain a listing of communications of which interception would be lawful. Such a listing might well be a useful part of the bill. We are saying that such a list should not be relied upon to correct fundamental defects in the wording of the general rule. We believe the proper approach is to amend the definition of "electronic communication" in the way suggested by Dr. Ellis and to amend the definition of "readily accessible to the public" as we recommended in our January 30 statement.

## PRIVACY PROTECTION AND ENCRYPTION TECHNOLOGY

At the January 30 hearing, Mr. Kastenmeier asked Mr. Amick and Mr. John W. Kelly of Southwestern Bell if--as ANARC had recommended--encryption should be the test of whether or not Federal penalities should come into play for violations of radio communications privacy. Mr. Amick replied:

> "We would say that encryption would be an added, user-supplied feature that would better protect his information transmission, but would not necessarily be the doorway to any prosecution efforts."

Lest this comment give the impression that AT&T planned to leave encryption to its customers, a copy of AT&T's announcement of an encrypted service for its cellular customers is attached (Attachment 4).

Another aspect of Mr. Amick's statement requires comment. Just prior to the sentence quoted above, he said:

> "Our position would be that subscribers to our services that are using services that are not intended for general broadcast to the general public should be entitled to a degree or an expectation of privacy, regardless of encryption devices used."

We would not dispute the claim that his customers should be entitled to a degree or an expectation of privacy, but we most certainly disagree that such an expectation deserves Federal protection in the absence of circumstances that justify the expectation. We further disagree that simply because a service is not intended for general broadcast, an expectation of privacy is reasonable. If in fact the service IS broadcast, as in the case of cellular radiotelephones, the intention (or lack thereof) can hardly matter.

During the hearing, Mr. George A. Kuhnreich of the Tandy Corporation stated that he had not seen any encryption devices sold for use with cellular phones, that such devices were not common, and that for:

> "...foolproof protection on a cellular mobile radio, we're talking in terms of three or four thousand dollars a unit."

His statement followed our audio demonstration and showing of a $7 integrated circuit that provides voice inversion (the lowest level scrambling) and a $40 microchip that provides digital encryption--the highest commercial-grade encryption available.

Attached (as Attachment 5) is a brief summary of a number of scrambling devices, available for under $800, for use with cellular radiotelephones. The price range is great ($7 to $795) because our list includes simple units as well as relatively sophisticated ones; book-size "black-boxes"; small circuit-boards meant to be installed in radios or telephones; and microchips meant to be designed into system circuitry. A typical "black box" unit is the "Priva-call sold in the District of Columbia by Cellular One and American TeleServices for $295 wholesale and $415 retail. Two units are required, one for the mobile radio and one for the landline.

In assembling this list--which is far from being comprehensive--we talked with many manufacturers and retailers who candidly discussed various aspects of their businesses. One volunteered that the only reason his device sold for as much as it did ($300) was because "...we have not met any resistance at all at that price." Another admitted that he could cut his price fifty percent and still make a profit. There seemed to be a clear consensus that if public demand for radio voice privacy increased significantly, it could "...become so cheap everyone would use it", as one sales manager put it.

## CELLULAR RADIOTELEPHONE MARKETING MISREPRESENTATIONS

We also talked to several manufacturers who had dropped out of the cellular market this past year. One explained "There is a false pretense that the people who market cellular tend to promote [about the security of their systems]."; "A good percentage of them took offense at the very question, because they try to convince everyone that there's no problem." Another manufacturer who is still in the marketplace complained that cellular companies are trying to "stifle" demand for low-cost voice protection by, on one hand, telling prospective customers it is not necessary, and on the other, promoting exorbitantly expensive encryption packages.

Intrigued by these comments, we investigated how several cellular service providers represented the question of call privacy to prospective customers. What we found confirmed the previous observations and revealed a shockingly pervasive misrepresentation of the actual interception vulnerability of cellular.

A sales representative for Bell Atlantic Mobile Systems in Washington, DC told us:

> "One of the beauties of cellular telephones is that it is completely private. It is actually more private than the landline we're speaking on right now.......if you're using the landline phones right now, you're using a less secure mode than cellular."

A customer service representative for Cellular One in Austin, Texas assured us that cellular was secure because the system:

> "...has [an] intense amount of scrambling that goes on.... I would say that the only people in the City of Austin that have the device to unscramble the cellular phones is probably the City of Austin Police Department Narcotics Division."

Similar statements were offered by EVERY cellular company we spoke to. We were only able to get information about devices like "Priva-call" when we specifically asked about such products by name. Often the person we talked with had to ask his or her supervisor to see if such devices even existed.

It is clear that the expectation of privacy in cellular comunications is actively cultivated by the companies, and is based on claims that are contrary to the facts. In the manner of a self-fulfilling prophecy, these FALSE EXPECTATIONS OF PRIVACY are now being used, by the cellular radiotelephone industry, as "evidence" of the need for the protection of H.R. 3378.

## CELLULAR TELEPHONE RECEPTION ON ORDINARY TV SETS

Perry Williams, Secretary of the American Radio Relay League, pointed out at the January 30th Subcommittee hearing that cellular telephone calls can be received on ORDINARY TELEVISION SETS. No scanner or other special equipment is needed because the system is totally open to casual interception.

Starting in the mid-1560s, the Federal Communications Commission required all new televisions to be capable of tuning up to UHF channel 83. This rule was in effect until 1982. When the cellular radiotelephone service was authorized by the Commission, TV channels 80 through 83 were assigned for its use. In their wisdom, the cellular companies used frequency modulation (FM) for their voice transmissions, just as television stations use FM for their sound. Thus, all televisions manufactured 1966-1982 can tune in on cellular phone calls on channels 80 through 83 just as clearly as if one were listening in on an extension phone.

Of course, since TV channels are much "wider" than cellular channels, one often hears more than one conversation simultaneously. But the sound quality is superior to FM cordless phones tuned in on amplitude modulation (AM) broadcast-band receivers. And, the range of cellular phones is much greater than cordless phones. While one might be able to hear a neighbor's cordless phone a few houses or blocks away, "cells" typically blanket up to 75 square miles (using an assumed cell radius of five miles) with both sides of a conversation being clearly audible.

The claim that moving from cell-to-cell means that only short segments of conversation can be intercepted is easily refuted with some simple calculations. If a cell is ten miles in diameter, and the mobile unit is traveling fifty-five miles per hour, it will be within the cell for up to twelve minutes; longer than the average phone call. If the unit is moving at ten miles per hour on average--which is more typical of in-city travel--it will be within the smaller in-city cell for a comparable time period. If it is standing still, which is often the case, it gets NONE of the so-called security provided by cell-switching.

In other words, the often-made claims that cellular radiotelephones are much more secure than cordless phones is utterly false. They are substantially LESS secure because there are many more receivers capable of tuning them in, these receivers are more modulation compatible than in the case of cordless phones, and the broadcast coverage area of cellular is many times larger. The vulnerability of cellular is profound and directly attributable to the way it is designed.

To demonstrate one way by which cellular radiotelephones might be protected from interception for more than a few seconds, we have attached (Attachment 6) a short article entitled "How To Improve

Cellular Security" from Mobile Phone News.

We urge the Subcommittee to investigate for itself whether the cellular radiotelephone industry is making unsubstantiated privacy claims to its customers and whether it is really in the public interest to commit Federal law enforcement funds and assets to protect the privacy of a radio service that ANY CHILD WITH A TELEVISION SET CAN INTERCEPT.

## QUESTIONABLE ABILITY TO ENFORCE PORTIONS OF H.R. 3378

We must question the statement by Mr. Kelly at the January 30 hearing that:

> "...there are sufficent penalties to deter that kind of activity--intentional interception--in place in the bill...."

Indeed, the technical situation suggests that NO AMOUNT of penalties in the bill will reduce the vulnerability of this particular type of system or offer realistic protection to its users.

Perhaps the most disturbing implication of his statement is that he seems to regard legal deterence as a substitute for his company's taking steps to protect the privacy of its customers, especially if those steps cost money. This is an unfortunate consequence of the present wording of H.R. 3378, which does not link Federal protection to any action on the part of the service provider. Similarly, Mr. Amick indicated that he thought the mere expectation of privacy was sufficient to entitle his company's customers to protection, irrespective of whether or not circumstances made those expectations

BEST COPY AVAILABLE

reasonable.

While we understand the Subcommittee's concern that loopholes in the present laws may impose a great uncertainty on communications providers about the legal status of their customer's transmissions, we must point out that the clear DANGER in H.R. 3378 is that it holds out the prospect of those providers being able to shift ALL COST AND RESPONSIBILITY for privacy protection onto the shoulders of the Federal Government (i.e. the public). The Federal Government would, in effect, be subsidizing these service providers to an untold degree, acting as the little Dutch boy responsible for plugging breaches in the rapidly growing network of leaky cellular dikes.

We have come to think of these new electronic communications providers as something akin to developers interested in building new housing at the edges of a city. They tell the city council "We'd love to do it, your citizens will get all this new housing and we can offer it to them fast and cheap. But ONLY if we don't have to put up walls. If people are concerned about privacy, they can build their own walls, or maybe the city can hire more police to keep the residents from looking at one another. It would just be too burdensome if we had to give them walls in addition to the many other wonderful features we can offer."

SUMMARY

The Association of North American Radio Clubs recommends six amendments to H.R. 3378 which we feel will substantially reduce our concerns about the potential adverse impacts of the bill. These amendments are summarized in Attachment 1.

We suggest that a listing of specific types of communications to be excluded from privacy protection under the bill, while perhaps useful, should not be a substitute to curing other inherent defects.

We have provided information on several types of available scrambling devices for cellular telephones (and other radio transmitters) which are well below the "three to four thousand dollar" price quoted by a cellular radiotelephone industry representative. More exhaustive research would probably discover hundreds of these devices, available at reasonable cost.

Our investigations into how cellular radiotelephone providers in the Washington, DC and Austin, Texas markets handled questions about cellular telephone privacy, revealed shocking misrepresentations which would lead members of the general public to expect privacy that cellular radiotelephones cannot provide.

We demonstrated that, despite claims to the contrary by the cellular industry, their transmissions are readily accessible in most every home in America, and are so easy to receive that a child can do it.

We restated our conviction that the prohibition against listening or intercepting WIRELESS communications is almost totally unenforceable. And further, that the cellular radiotelephone industry is attempting to shift the responsibility and cost for privacy protection from their own shoulders--where it belongs--to those of the Federal Government.

We have NEVER argued that anyone has the right to eavesdrop on private conversations. We do argue that--just as the FCC says--those who transmit their private information on the public's airwaves over a broad and populated area bear the responsibility for protecting whatever information they do not want the public to intercept.

It is not the public's duty to clean away every carbon-paper, that may disclose a credit card number, left in a restaurant ashtray. It is not the duty of the Federal Government to subsidize new communications technologies at any cost.

It is not the right of the cellular radiotelephone industry to impose an expectation of privacy so unreasonable that it deprives others of access to the public domain.

It IS the right and the duty of Congress to consider facts--not rhetoric--and the public good when passing PUBLIC laws. We ask that it do no less on H.R. 3378.

**ASSOCIATION OF NORTH AMERICAN RADIO CLUBS**

RECOMMENDED AMENDMENTS
TO
H.R. 3378
ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985
FEBRUARY 27, 1986

AMENDMENT ONE. Section 2510 of title 18, United States Code should be amended by striking out paragraph (1) and inserting the following:

> "(1) 'electronic communication' means any communication made in whole or part through the use of facilities for the transmission of signs, signals, writing, images, sounds, data or intelligence of any nature in whole or in part by wire, radio, electromagnetic or photoelectronic system that affects interstate or foreign commerce where the person originating such communication exhibits an expectation that such communication is not subject to interception under circumstances justifying such expectations."

This amendment would provide for uniformity in applying the same "reasonableness test" to electronic communications that is applied to oral communications.

AMENDMENT TWO. Section 2510(4) of title 18, United States Code should be amended by striking out the word "aural" from the

**Attachment 1**

definition of "intercept", providing the following definition:

> "(4) 'intercept' means the acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."

This amendment would remove any ambiguity inherent in using a derivation of a word--in this case "interception"--in its definition.

AMENDMENT THREE. Section 2510 of title 18, United States Code should be amended by adding at the end the following:

> "(12) 'readily accessible to the public' means that an electronic communication (i) is transmitted in an unscrambled or unencrypted manner; (ii) shares a common modulation type with other signals; and (iii) has a wide coverage area so as to be receiveable in populated places."

This amendment provides a definition for one of the KEY PHRASES in H.R. 3378.

AMENDMENT FOUR. Section 2511(2) of title 18, United States Code should be amended by adding at the end the following:

> "(g) It shall not be unlawful under this chapter for any person --
>
> > "(ii) to intercept any electronic communication which is transmitted--
> >
> > > "(IV) in an unscrambled or unencrypted manner."

This would make it clear that electronic communications which are not scrambled or encrypted--implying that scrambling or encryption is a test for the intention of privacy--are not protected from interception.

This amendment is a modification of Amendment Two offered in ANARC's January 30, 1986 statement to the House Subcommittee on Courts, Civil Liberties and the Administration of Justice. This modification is necessary so that the H.R. 3378 change to Section 2511(2) shown on page 2, lines 20 through 25 of the bill would not require amendment.

AMENDMENT FIVE. Section 2511(2) of title 18, United States Code should be amended by adding the following:

> "(g) It shall not be unlawful under this chapter for any person --
>
> > "(iv) to manufacture, sell, purchase, possess or use any type of radio communications receiver for non-criminal purposes."

Rhetoric surrounding H.R. 3378 suggests that language attempting to limit radio communication receivers may be forthcoming. This amendment simply reaffirms existing United States public policy.

AMENDMENT SIX. Section 2511(2) of title 18, United States Code should be amended by adding the following:

> "(g) It shall not be unlawful under this chapter for any person --
>
> > "(v) to intercept any electronic communication causing harmful interference to any lawfully operating station."

This amendment removes privacy protection from electronic communications where such protection would make it impossible to identify and take actions to remove the interfering signal.

## Proposed Changes in Wording of S. 1667
## and
## Reasons for Changing

### Sec. 101 FEDERAL PENALTIES FOR THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS

### 1. Definition of the Term "Electronic Communication"

The proposed definition is as follows:

"'electronic communication' means any transmission of signs, signals, writing, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, or photoelectric system that affects interstate or foreign commerce."

#### a. "Photoelectronic System" Rather Than "Photoelectric System"

Recommended additional language:

"'electronic communication' means any transmission of signs, signals, writing, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, or ~~photoelectric~~ photoelectronic system that affects interstate or foreign commerce." (Underscore indicates language to be added, strikeover indicates language to be deleted.)

In physics, the word "photoelectric" refers narrowly to the ejection of an electron from a solid by an incident photon. The word "photoelectronic" refers to the combining of the technologies of optics and electronics, which is the intention of the definition.

#### b. Inclusion of Radio Transmissions Within the Definition of "Electronic Communication"

Since the definition of the term "electronic communication" includes radio transmissions, the interception of which are also covered by Section 705 (previously numbered Section 605) of the Communications Act, how will the jurisdiction of each act be delineated to avoid contradictory results?

For example, the Communications Act requires that the intercepted radio communication be also divulged and published; Section 2511(1)(a) of the Wiretap Law as amended by this Act only requires that the electronic communication be intercepted.

**Attachment 2**

c. Addition of Language from Current Wiretap Law Definition of "Wire Communication" (Sec. 2510 (1))

Recommended additional language:

"'electronic communication' means any communication made in whole or in part through the use of facilities for the transmission of signs, signals, writing, images, sounds, data or intelligence of any nature ~~in whole or in part~~ by a wire, radio, electromagnetic, or [photoelectric] [photoelectronic] system that affects interstate or foreign commerce." (underscore indicates language to be added, strikeover indicates language to be deleted.)

The additional language is more consistent with the current defintion of wire communication; this means that judicial interpretations applied to the earlier definition may be more easily used as precedent for the new definition. The additional language, however, in no ways limits the more varied forms of communication that the new definition is intended to encompass.

Including the phrase "use of facilities" emphasizes that the protections are applying to the communications systems rather than the communications contained within the system, stressing the fact that the means of communication and not the content are being regulated. This helps to avoid potential conflicts between the 1st Amendment rights for free speech and trying to regulate (and possibly having to monitor) communications.

d. Addition of Language from Current Wiretap Law Definition of "Oral Communication" (Sec. 2510(2))

"'electronic communication' means any [communication made in whole or part through the use of facilities for the] transmission of signs, signals, writing, images, sounds, data or intelligence of any nature [in whole or in part] by wire, radio, electromagnetic or [photoelectric] [photoelectronic] system that affects interstate or foreign commerce where the person originating such communication exhibits an expectation that such communication is not subject to interception under circumstances justifying such expectations." (Underscore indicates language to be added.)

The expectation of privacy language added at the end of the definition is consistent with the language currently employed in the definition of "oral communication" in Section 2510(2) and U.S. Supreme Court decisions on privacy issues. If it is to be excluded, it is critical that the legislative history provide some rationale as to why:

- The "reasonable expectation of privacy test" is not to be applied to "electronic communications," but is to be applied to "oral communications."

- "Electronic communications" are to have absolute protection, unless subject to one of the stipulated exceptions.

## 2. Definition of the Word "Intercept"

The proposed amendments to the current definition are as follows:

> "'intercept' means the ~~aural acquisition~~ interception of the contents of any ~~wire~~ electronic or oral communication through the use of any electronic, mechanical, or other device." (Strikeover indicates language to be deleted, underscore indicates language to be added.)

Our recommendation is that the definition of the word "intercept" be deleted, and that the "plain meaning" control, as in Section 705 of the Communications Act. The proposed definition would seem to require that the "plain meaning" of the word "interception" will control.

If the word "intercept" is to have a definition, we would recommend that in the proposed definition the word "interception" be changed to "unauthorized acquisition," and that additional language be added to avoid limiting the interception to "through the use of any electronic, mechanical, or other device."

> "'intercept means the ~~interception~~ unauthorized acquisition of the contents of any electronic or oral communication through the use of any electronic, mechanical, or other device or other technological means of interception." (Strikeover indicates language to be deleted, underscore indicates language to be added.)

## 3. Lack of Definitions for the Terms "Access," "Electronic Communication Systems," "Electronic Communication Services," "Provider of Electronic Communication Services," and "User of Electronic Communication Services"

S. 1667 does not contain any definitions for the above terms. At this time, we would like to propose the following definition for the word "access":

> "'access' means to instruct, interact or communicate with, intercept, or otherwise make use of any resources of an electronic communication system."

2-3

4. Exceptions With Respect to Electronic Communications

   a. Proposed Section 2511(2)(g)(i)

   > "(g) It shall not be unlawful under this chapter for any person--
   >
   > (i) to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public."

   What does "readily accessible" mean? What would be the difference between "readily accessible" and "accessible"?

   b. Proposed Section 2511(2)(g)(ii)(II)

   > "(g) It shall not be unlawful under this chapter for any person--
   >
   > .
   >
   > .
   >
   > (ii) to intercept any electronic communication which is transmitted--
   >
   > .
   >
   > .
   >
   > (II) by walkie-talkie, or a police or fire communication system readily accessible to the public.

   Same problem with "readily accessible" as described in "a." above. The term "walkie-talkie" is a layman's term, is technologically restrictive, is covered by the proposed Section 2512(2)(g)(i) ("an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public"), and can be deleted.

SECTION 1. SHORT TITLE

5. Proposal to Change Title of Act from "Electronic Communications Privacy Act of 1985" to "Electronic Surveillance Act of 1985"

   For the reasons given below, we recommend changing the title to "Electronic Surveillance Act of 1985."

   - The term "Electronic Surveillance" rather than "Electronic Communications Privacy" is more representative of the issues addressed in the provisions of this Act and the Wiretap Law, which it amends.
   - The major purpose of the provisions is to regulate the circumstances under which government agencies may conduct electronic surveillance upon electronic communications systems.

- Privacy is not the main thrust. The most widely quoted recent definition of privacy is probably Alan Westin's: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

The provisions of this Act do not provide controls over "when, how, and to what extent information... is communicated." Rather, it seeks to provide protections to the electronic communications systems so that when a communication is made, there will not be any unauthorized interception. This Act attempts to control the communication systems, not the communications contained within the systems.

Note: an advantage of emphasizing the providing of protections to the electronic communications systems rather than the communications contained within the systems, is that it avoids potential conflicts between the 1st Amendment rights for free speech and trying to regulate (and possible having to monitor) communications.

MICRO
WAVE
NEWS

Vol.V No.3 A Monthly Report on Non-Ionizing Radiation April 1985

**INSIDE...**

HIGHLIGHTS pp 2-4

IBM Report Recommends Shielding Older VDTs

Confusion over EPA ELF Research

Power Line Studies at IEEE PES Meeting

High School Student on PEMF Effects

EXCERPTS pp 5-8

FCC's Rules on RF Hazards Under the National Environmental Policy Act

FROM THE FIELD p 11

Dr. Bill Guy's Recommendations to IBM on VDT Radiation

Letter from EPA's Sheldon Meyers to New Jersey's Department of Environmental Protection

UPDATES pp 8-11

FAA and RTCA on Aircraft EMI □ Opposition to EMPRESS II □ IEC on Industrial EMC Standard □ Magnetic Measurements □ FDA Bulletins Back in Print □ Radar Detectors □ Microwave Drying □ Australian VDT Radiation Measurements □ First Cuban Interference Claim □ NBS to Study EMI Test Methods □ Ultrasound and Chromosomal Effects □ Moscow Bugs □ VDT Legislation □ SAE AE-4 & ANS C63 Meetings □ IEEE Special Issue on Radar □ Power Line Freak Accidents □ Japanese HPS Meeting □ and more...

Classifieds p 12

*Microwave News* invites contributions to *From the Field* our occasional column featuring news and opinions from the non-ionizing radiation community Letters from readers are also welcome

## FCC To Consider RF/MW Radiation Hazards

The Federal Communications Commission (FCC) has decided to require its applicants to consider the health risks associated with human exposures to radiofrequency and microwave (RF/MW) radiation emitted by certain types of communications facilities At the same time, the commission has begun the process of fine-tuning the new rules by proposing to include and exclude specific classes of communications facilities

The rules amend existing FCC regulations for compliance with the National Environmental Policy Act of 1969 (NEPA), which requires the preparation of environmental impact statements (EIS) for "major" federal actions With respect to non-ionizing radiation, the agency will now define a major action as any facility, new or upgraded, which "would expose workers or the general public to levels of RF radiation exceeding health and safety guidelines issued by the American National Standards Institute" (ANSI)

Under the rules, which will take effect on October 1, applicants for construction permits, licenses or renewals as well as those seeking to modify existing facilities, would have to evaluate radiation hazards If a project qualifies as a major action, with human exposures above the ANSI limits, a narrative statement describing the environmental conditions would have to be submitted to the commission The FCC would then decide if an EIS is required

In a series of telephone interviews, knowledgeable sources indicated that the net effect of the new FCC rules would be the enforcement of the

*(continued on p 4)*

## AIBS ELF Study Completed

The American Institute of Biological Sciences (AIBS) has concluded that it is "unlikely" that the extremely low frequency (ELF) electric and magnetic fields associated with the Navy's Project ELF submarine communications system can lead to adverse health effects on the public, animals or plants

Professor H B Graves of Pennsylvania State University in University Park, the chairman of the AIBS panel, told *Microwave News* that the committee was unanimous in reaching its conclusions and recommendations

The U S Navy, which commissioned the study, plans to release it on April 1 In late March, Graves briefed legislators on Capitol Hill in Washington, DC, and state officials in Madison, WI, and Lansing, MI, on the study findings

The Navy prepared a 38-page appendix to the 290-page AIBS report that details the characteristics of the electromagnetic fields associated with the ELF system

News of the release of the AIBS study comes as we go to press We will present a detailed summary of the report in our May issue

Attachment 3

## HIGHLIGHTS

under HVAC Transmission Lines," (85 WM 224-1). Using computer simulations, Dr. Don Deno of General Electric and Mike Silva of Enertech evaluated the likelihood of fuel ignition caused by sparks during refueling for various types of trucks and automobiles along the right-of-way (ROW) of a 500 kV line. They found that the risk for an automobile is less than one in a trillion. The greatest probability is for a trailer truck on a blacktop road: approximately one in seven million. If a spark were to cause ignition, an explosion would be very unlikely, the researcher found.

- "Testing of Railroad Signal Equipment for Power Line Interference Susceptibility Part I: The Test Jig" (85 WM 113-6) and "Part II: Test Results" (85 WM 114-4). Much of this work has already been reported (see *MWN*, September and December 1983). Allen Taflove, formerly with IITRI and now an associate professor at Northwestern University in Evanston, IL., John Dunlap of the Electric Power Research Institute and Raymond Zalewski of IITRI advise utilities "to work with the railroads to set up measurement procedures (or procurement standards) to test each item of vital railroad signal equipment that may be subjected to AC interference. Both safe failures and false clear failures should be tested."
- "Measurement and Statistical Analysis of Ozone from HVDC and HVAC Transmission Lines," (85 WM 226-6). A team from Hydro-Quebec and its research institute (IREQ) led by L. Varfalvy found that, in most cases, a 735 kV AC line had negligible effects on ambient levels of ozone. Even in worst case situations, the maximum contribution of the power line will not exceed 5-10 parts per billion along or near the ROW. For a ± 900 kV DC line during bad weather conditions, the maximum contribution to ozone levels could be quite significant.
- "Analysis of Effect of Shield Wires on Electrostatic Induction by AC Transmission Lines," (85 WM 223-3). A group of Japanese researchers has devised a model for the effectiveness of shield wires on the ground level electric field. Measured values were in good agreement with the group's calculations.
- "Exposure to Transmission Line Electric Fields During Farming Operations," (85 WM 225-5). Mike Silva and Dennis Huber of Enertech have estimated the exposures experienced by farmers whose property is crossed by various types of power lines. For instance, for a 765 kV line, a farmer would spend about 20 hours a year in fields above 3 kV/m and one hour in fields above 8 kV/m. They note that the cabs of most farm machinery shield workers to a level of five percent of the unperturbed electric field outside the cab.

Single copies of the above papers are available for $3.00 (IEEE members), $6.00 (others) from: Single Publication Sales Dept., IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854.

A tutorial on "Power System Harmonics," held at the PES meeting, was well attended, attracting about 75 participants. The course text (84 EH0221-2-PWR) is available for $8.00 (IEEE members), $16.00 (others).

## FCC on Radiation Hazards

(continued from p. 1)

ANSI standard. The time and effort needed to prepare an EIS is such that most applicants will design their facilities to comply with the ANSI limits, one FCC staffer said.

Indeed, an FCC attorney told *Microwave News* that since NEPA became law in 1969 the commission has written fewer than six EIS's. None of these addressed RF/MW radiation.

### Technical Bulletin

The FCC is preparing a technical bulletin to help evaluate compliance with the new rules. According to Dr. Bob Cleveland of the commission's Office of Science and Technology, the bulletin will help broadcasters predict field strengths from antennas and will review measurement procedures. Cleveland said that the bulletin would be updated as needed. He also said that the commission will consult with staffers at the Environmental Protection Agency (EPA) in developing the bulletin. In addition, the National Association of Broadcasters has offered its assistance.

In adopting the radiation rules, the FCC acknowledged the absence of federal standards but argued that, "We believe the fact that there are currently no mandatory federal standards for exposure of the public to RF radiation does not excuse us from our obligations under NEPA to evaluate the FCC actions for significant environmental impact."

The new rules will apply to: (1) radio and television broadcast stations, (2) experimental broadcast stations including radio transmitters, (3) low-power television stations and (4) transmitting satellite earth stations.

In a separate action, the FCC proposed to exclude categorically land-mobile transmitters and microwave point-to-point relay links from the NEPA requirements. The commission also proposed to apply the rules to shipboard satellite earth terminals. In so doing, the commission asked interested parties to respond to a series of questions on worst case exposures, field strength prediction models, measurement methods and other related issues.

### No Federal Preemption

In explaining its decision, the FCC noted that:

- Though standards more restrictive than ANSI's are being proposed and adopted by national and international organizations, the commission decided not to wait for the "ultimate standard," but to act on the basis of the available record. The commission advised that "we may revisit this issue and recommend use of a different standard in the future."
- Though a number of commenters called for the agency to quash the movement towards state and local safety standards in the absence of federal rules, the commission said that, after having given the matter "serious consideration," it had decided not to resolve the issue of federal

preemption at this time. But it warned that, "Should non-federal RF radiation standards be adopted, adversely affecting a licensee's ability to engage in commission-authorized activities, the commission will not hesitate to consider this matter at that time."

- Though the FCC had originally proposed to key its actions under NEPA to the Occupational Safety and Health Administration's (OSHA) 10 mW/cm$^2$ standard, because the OSHA standard was based on the old ANSI standard, which was revised in 1982, the commission decided to base its rules on the more recent guidelines.

Dr. Robert Powers, FCC's chief scientist, will outline the new rules at a panel discussion on non-ionizing radiation at the *Annual Convention of the National Association of Broadcasters* in Las Vegas, NV, the week of April 14. And Cleveland will address the rules at the May 14-17 *Annual Meeting of the Electromagnetic Energy Policy Alliance* in San Diego, CA. Excerpts of the FCC's "Report and Order" appear below.

The FCC began considering radiation hazards in 1979 when it issued a Notice of Inquiry (NOI). In February 1982, the commission proposed the rules which it has now adopted with some revisions (see *MWN*, March 1982). Nineteen organizations filed comments and reply comments on the FCC's proposal (see *MWN*, September 1982). Comments on the new proposal are due on June 19, with reply comments due on July 19.

The "Report and Order" appears in the March 20 *Federal Register*, (50 *FR* 11151), and the proposed revision appears in the March 18 *Register* (50 *FR* 10814). For more information, contact FCC's Cleveland at (202) 632-7040 or Stephen Klitzman at (202) 632-6405. ●

# EXCERPTS

## FCC's RF Human Exposure Rules Under NEPA

*Reprinted below are excerpts from the Federal Communications Commission's (FCC) rules to consider radiofrequency (RF) hazards under the National Environmental Policy Act (NEPA). All footnotes have been deleted from the original FCC text, which appeared in the March 20* Federal Register *(50* FR *11151). These rules are part of FCC's General Docket No. 79-144. They were adopted on February 26 and released on March 14.*

### Summary

1. The Commission is amending Part 1 of its rules implementing the National Environmental Policy Act of 1969 (NEPA), 42 U.S.C. 4321 *et seq.* (1976). The amendment provides for environmental analysis of major Commission actions that may result in non-compliance with applicable health and safety guidelines for radiofrequency (RF) radiation. Our processing guideline for determining the significance of human exposure to RF radiation will be the "Radio Frequency Protection Guides" adopted in 1982 by the American National Standards Institute (ANSI). At this time, the rule amendment will only apply to major actions taken by the Commission with respect to the following facilities authorized by the FCC Rules and Regulations: (1) broadcast facilities authorized under Part 73, (2) broadcast facilities authorized under Part 74 (Subparts A and G only); (3) satellite-earth stations authorized under Part 25, and (4) experimental facilities authorized under Part 5. An accompanying *Further Notice of Proposed Rule Making*, also being issued today, proposes to categorically exclude other FCC-regulated facilities and operations from the provisions of this rule, except for shipboard satellite-earth terminals.

### II. Background

2. On June 7, 1979, the FCC issued a *Notice of Inquiry* (NOI) concerning the responsibility of the FCC to consider biological effects of radiofrequency (RF) radiation when licensing facilities and authorizing equipment that utilize RF energy.

3. As a result of the comments received in response to the FCC's NOI and our assessment of the Commission's statutory responsibilities under NEPA, the Commission issued a *Notice of Proposed Rule Making* (NPRM) on February 18, 1982, proposing that applications for equipment authorizations would be treated as "major actions" triggering environmental assessment when the equipment in question did not comply with RF radiation emission standards. It was also proposed that applications for construction permits or licenses to transmit would be treated as "major actions" triggering environmental assessment when the proposed operation would result in the exposure of workers or the general public to levels of RF radiation in excess of safe levels established by federal agencies which have jurisdiction to set such standards.

### III. Discussion

**A. General**

4. A total of twenty three filings of comments and reply comments was received at the FCC in response to the Commission's NPRM in Docket 79-144. The respondents included individuals, broadcast groups, major corporations, trade associations, a labor union, local government officials, and the U.S. Environmental Protection Agency (EPA).

5. With a few exceptions, respondents to the NPRM generally supported the thrust of the Commission's proposal. The general tone of the comments indicated a desire by many respondents that the Commission clearly establish a policy regarding RF radiation hazards and clarify Commission and licensee responsibilities in this area of growing public concern. Several of the respondents also suggested the Commission take actions that, we believe, go beyond the scope of this proceeding. Although various broadcast groups, such as the National Association of Broadcasters (NAB), the TV Broadcasters All Industry Committee (TVBAC), the Association for Broadcast Engineering Standards, Inc. (ABES), and the National Association of Public Television Stations basically supported the proposed rule, they and others urged the Commission to issue a policy statement dealing with federal preemption of local and state standards for RF radiation.

6. Two respondents felt that the Commission should not adopt the proposed rule amendment at this time. The Utilities Telecommunications Council (UTC) recommended "that the Commission postpone adoption of its proposal until the EPA or another responsible federal agency establishes a legally enforceable exposure standard." UTC felt that it would be premature for the

# AUTOPLEX Cellular Privacy Data Product

### *Responding to Your Customers' Needs*

Development of the AUTOPLEX System Privacy/Data Product is based on the increasing number of current and future business, military and government cellular phone users openly concerned about the total privacy of their phone conversations and the security of data transmitted through the airwaves

Offered on a system-wide or per customer basis, this AUTOPLEX System service makes use of Switch Resident Equipment (SRE), an AT&T Information Systems CTS 1620 Privacy/Data Accessory, and Key Modules It offers three types of calls — mobile-to-land, land-to-mobile and mobile-to-mobile — plus a wide selection of customer features

Both privacy and data applications will appeal to all levels of executives, government officials, professionals, military personnel, sales and service representatives plus all other cellular phone users wishing to protect their conversations

The data security application can be used to access remote databases, such as stock market information, insurance databases, or order and inventory data bases No special equipment is needed at the destination being accessed, a definite competitive advantage

### *Voice Privacy Benefits*

For service providers, Voice Privacy can allow current customers to discuss sensitive issues thereby increasing air time It can also provide you with service differentiation to attract new corporate and government customers The premium charge billed can generate increased system revenues For customers, there is an increased level of privacy plus the capability to call any destination — privately — without the need for destination apparatus

### *Data Security Benefits*

Service providers can take advantage of service differentiation, additional air time for data calls, premium billing and the opportunity to interest new users with specific data applications, e g field sales or service, order entry, stock checking and electronic mail

Customers equipped with their own data terminals can receive data transmissions in their vehicles, protect access codes, passwords and sensitive information, call anywhere without special destination equipment, avoid hand-off and fading problems through error-free transmission, and save time using data speeds of 300/1200/2400 BPS

### *System Configuration*

**Switch Resident Equipment (SRE):** The SRE consists of System Channel Units (SCUs), Data Sets and a Common Control Processor Connected to trunks in an AUTOPLEX Mobile Telephone Switching Office, SCUs are compatible with four-wire E&M Type I and II trunks The SRE responds to requests for private voice and data services activated through signaling tones and interfaces with trunk and signaling circuits For data service, SCUs provide the capability to communicate with computer modems

An optional Common Control Processor (required for systems with more than 48 System Channel Units) consists of terminals, two key processors and two operations processors This equipment provides for secure dial back, remote equipment testing, SCU software download, class-of-service record, encryption-key usage records and administration of up to 500,000 encryption keys

**CTS 1620 Accessory:** This unit is placed in a cellular phone user's trunk or passenger compartment and is connected to a cellular phone at the standardized interface between the control unit and transceiver unit It communicates with the cellular phone and encrypts digitized voice signals to provide private voice service Asynchronous data signals are also encrypted to provide data service **Both services use a** Proprietary Digital Encryption Protocol

**Key Modules:** Two modules containing encryption keys can be used The fixed key module contains an encryption record used between the CTS 1620 and the SRE for privacy and data The configuration/key module can hold a private encryption record used for end-to-end privacy and data

AT&T

Attachment 4

**ASSOCIATION OF NORTH AMERICAN RADIO CLUBS**

## LOW-COST SCRAMBLING DEVICES FOR CELLULAR RADIOTELEPHONES

CELLULAR ONE (8755 Walker Drive, Greenbelt, MD 20770; (301) 441-2701). This company sells the "Priva-call" scrambler (see Attachment) for $295 per unit wholesale. It comes in two versions; one designed for mobile units, the other for base installation. Each is a self-contained box measuring about 5 1/2" wide by 1 1/2" high by 9 1/2" deep. Each plugs into the phone circuit with a simple wire and jack interconnection. Cellular One claims the unit is only compatible with Motorola cellular radiotelephones and landline phones, but the manufacturer of the devices, MEICO, says this is just to encourage Motorola sales. The unit apparently works with any cellular phone. "Priva-call" devices are sold retail by American TeleServices (6500 Rock Springs Drive, Bethesda, MD; (301)597-0800) for $415 each.

CONTROLONICS, INC. (P.O. Box 568, Westford, MA 01886; (617) 692-5434). This company makes four scrambling devices: two designed for use with two-way radios and two for use with telephones. The radio and the telephone devices are compatible with each other, so various combinations can cover conversations over wire or wireless, or circuits combining both. The "Telecode One" unit retails for $749 per unit. Housed in a box designed to fit under a desk telephone, it

Attachment 5

interfaces with the phone through a standard phone jack. It communicates with a similar unit, or with the "FDS-100" unit, designed for radio, which retails for $395. Both devices use voice inversion. Much higher security can be obtained from their other two devices, the "Telecode Three" which retails for $595 and the "FDS-300" which retails for $795. These use a nonlinear swept-inversion type of scrambling with the inversion center-frequency changing thirty-one times per second.

MIDIAN ELECTRONICS [2302 East 22nd Street, Tucson, AZ 85713; (602) 884-7981]. The "VPU-1" is a small circuit-board that retails for $199. It provides full duplex voice inversion, and can be built into a radiotelephone or added on. In large lots, there is a discount of "about 25 percent." Planned for release later this year is the "VPU-3" which is expected to provide the same capability at a lower cost.

MX-COM, INC. [4800 Bethania Station Road, Winston-Salem, NC; (919) 744-5050]. This company makes integrated circuits for two-way radios. Three voice security microchips are currently under development, representing three degrees of sophistication, with somewhat different applications. All are in the $10 to $20 price range for single copies.

RESEARCH ELECTRONICS, INC. [1570 Brown Avenue, Cookeville, TN 38501; (800) 824-3190]. Model "ACS-2", introduced in August, 1985, is a one-piece, acoustic-coupled device retailing for $299 per unit. In addition to supplying voice inversion scrambling, at the onset of a call, the device has an automatic "handshake" procedure that verifies that both parties are authorized to descramble each other's transmissions. The device mounts on the telephone handset; no wire connection is required.

STANDARD MICROSYSTEMS [35 Marcus Boulevard, Hauppage, NY 11788; (516) 273-3100]. We submitted information on the company's $7 "COM9046" voice inversion integrated circuit with our Janaury 30, 1986 statement. Mr. Jocques Hakim of the Company informed us that over a dozen radio, telephone and cellular companies have purchased batches of the microchip for experimental development of products incorporating it. AT&T was said to be one of the companies. Mr. Hakim's impression is that Webcor may be the first to introduce a cellular radiotelephone using the chip, possibly as early as this year.

TRANSCRYPT INTERNATIONAL, INC. [1440 Buckingham Drive, Lincoln, NE 68506; (402) 483-2961. The "SC-400" is a hybrid thick-film circuit about the size of two postage stamps (1.53 by .83 inches) designed to fit inside a radio or phone housing. It offers voice inversion with four programmable coding sequences. Single copies retail for $158.50; in batches of one thousand, they are "under 100 dollars." An add-on device, the "SC-450", will be announced in April, and "could be made available for the same prices." The "SC-450" will be a substantial improvement in security, using a rolling-code voice inversion with several thousand possible codes.

# Priva-Call Scrambler

Keeps your car phone conversations private. The Priva-Call Scrambler helps prevent car phone eavesdropping by scrambling your conversations while they're being transmitted—on the air waves *and* on the telephone land lines. Two Scramblers are needed to ensure privacy—one for your cellular car phone, the other for a land line phone.

Affordable. The Priva-Call Scrambler is very affordable compared to the high-priced, high security scramblers which can cost you twice as much.

Extra Security. The Priva-Call Scrambler offers you a choice of 25 identification codes to further ensure your privacy. It operates on simple frequency inversion scrambling, so the new 800 MHz scanner is incapable of hearing your cellular conversation.

While Cellular One distributes the Priva-Call Scrambler in an effort to provide privacy, it is not ensured or guaranteed.

*The Washington/Baltimore Cellular Telephone Company*
**CELLULAR ONE**
*Innovators of Cellular Communication*

## PEOPLE

● The FCC's highest award for distinguished service at the commission, the Gold Medal for 1985, was presented to Daniel Armstrong, associate general counsel/litigation, and Albert Halprin, chief, common carrier bureau. Claudia Pabo, deputy chief, common carrier bureau policy and planning division; Ron Lepkowski, chief, common carrier bureau satellite radio branch; and CLyde Whitlock, chief, office of managing director, operations support division, services and supply branch received the silver medals, signifying meritorious service.

● The board of directors of Ericsson Inc. has elected Bjorn Svedberg company chairman He will continue his duties as chief executive officer and president of LM Ericsson. In addition, to "further demonstrate Ericsson's commitment to the U.S. telecommunications market" the board announced that a U.S. executive will be named president of Ericsson Inc., headquartered in Richardson, Texas.

● Jerrold Adams, former manager at AT&T Information Systems Inc., has been named president of the New York City market's nonwireline system. Adams will be responsible for starting up Cellular Telephone Co.'s New York service--expected to be up in the first quarter of this year (MPN, Dec. 25, 1985, p. 6).

● Several recent promotions and appointments have taken place at Quintron Corp. Neil Quellhorst has been appointed vice president of engineering; Clark Emerick has been named cellular product manager; Brian Cox has been promoted to executive-level engineering professional, and Scott McFarland has joined Quintron as lead engineer.

● The Antenna Specialists Co. has promoted 4 people in its marketing department. Alex Dolgosh has been named director of marketing; Robert Levy has been promoted to sales manager, national accounts; Patricia Fritz has been named the company's new Western regional manager, and Kim Goryance has been promoted to Eastern regional manager.

## COMMENTARY

### HOW TO INCREASE CELLULAR SECURITY

By Stuart Crump Jr., Founding Editor
CELLULAR RADIO NEWS

Is your cellular phone call secure? Congress is toying with legislation that would make it illegal to eavesdrop on radiotelephone calls--a new law that does about as much to guarantee your privacy as dressing with your window shades open.

One answer to cellular privacy is to use some sort of encryption, but scramblers are expensive--from $500 to $5,000 or more.

With their frequent hand-offs and low power, cellular calls enjoy a high level of security already, but that security is gradually decreasing as 800 MHz scanners become more popular among electronic voyeurs.

Instead of trying to sidestep the privacy issue by lobbying for an unenforceable law, the cellular industry should come up with its own way to offer a higher degree of security. Here's an idea that might work with a slight modification to the MTSO software:

Instruct the central switch to "hand off" in-progress cellular calls more frequently, perhaps every 10 seconds or so. Hand-offs occur when the cellphone moves between cells, but there is no reason why a hand-off couldn't be made from one frequency to another within a single cell. The military has been using a similar type of frequency hopping to secure its transmission for many years.

Frequent hand-offs would frustrate the scanner-hobbyist crowd and make cellular calls almost 100% secure. The carrier could charge a slight premium for this higher security, thus bringing in additional revenues with no additional expense in equipment.

The ultimate solution is to go to digital, but until we do, frequency hopping offers an inexpensive interim solution to the question of cellular privacy.

Attachment 6

NINETY-NINTH CONGRESS

PETER W. RODINO, JR., NEW JERSEY, CHAIRMAN

JACK BROOKS, TEXAS
ROBERT W. KASTENMEIER, WISCONSIN
DON EDWARDS, CALIFORNIA
JOHN CONYERS, JR., MICHIGAN
JOHN F. SEIBERLING, OHIO
ROMANO L. MAZZOLI, KENTUCKY
WILLIAM J. HUGHES, NEW JERSEY
MIKE SYNAR, OKLAHOMA
PATRICIA SCHROEDER, COLORADO
DAN GLICKMAN, KANSAS
BARNEY FRANK, MASSACHUSETTS
GEO. W. CROCKETT, JR., MICHIGAN
CHARLES E. SCHUMER, NEW YORK
BRUCE A. MORRISON, CONNECTICUT
EDWARD F. FEIGHAN, OHIO
LAWRENCE J. SMITH, FLORIDA
HOWARD L. BERMAN, CALIFORNIA
FREDERICK C. BOUCHER, VIRGINIA
HARLEY O. STAGGERS, JR., WEST VIRGINIA
JOHN BRYANT, TEXAS

HAMILTON FISH, JR., NEW YORK
CARLOS J. MOORHEAD, CALIFORNIA
HENRY J. HYDE, ILLINOIS
THOMAS N. KINDNESS, OHIO
DAN LUNGREN, CALIFORNIA
F. JAMES SENSENBRENNER, JR., WISCONSIN
BILL McCOLLUM, FLORIDA
E. CLAY SHAW, JR., FLORIDA
GEORGE W. GEKAS, PENNSYLVANIA
MICHAEL DeWINE, OHIO
WILLIAM E. DANNEMEYER, CALIFORNIA
HANK BROWN, COLORADO
PATRICK L. SWINDALL, GEORGIA
HOWARD COBLE, NORTH CAROLINA

**U.S. House of Representatives**
**Committee on the Judiciary**
**Washington, DC 20515**
**Telephone: 202-225-3951**

GENERAL COUNSEL
M. ELAINE MIELKE

STAFF DIRECTOR
GARNER J. CLINE

ASSOCIATE COUNSEL
ALAN F. COFFEY, JR.

February 19, 1986

The Honorable Edwin Meese III
Attorney General of the United States
United States Department of Justice
Washington, D.C. 20530

Dear Mr. Attorney General:

The Subcommittee on Courts, Civil Liberties and the Administration of Justice, which I chair, is holding hearings on H.R. 3378, the Electronic Communications Privacy Act of 1985. The purpose of this bill is to extend the protection of the Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968) to new communications technologies.

The Subcommittee is interested in obtaining the opinion of the Department of Justice on the status under current law of willful unauthorized interception of certain telephone calls, specifically:

(1) between cellular and landline telephones;
(2) between two cellular telephones;
(3) between cordless and landline telephones; and
(4) between two cordless telephones.

In addition, it would be useful to know whether the Department would consider an advertisement promoting the use of a device for such interception to be a violation of 18 U.S.C. 2512(1)(c)(ii). For your reference, I have enclosed a copy of an advertisement that has been made a part of the Subcommittee's hearing record, as well as a second advertisement recently provided to the Subcommittee.

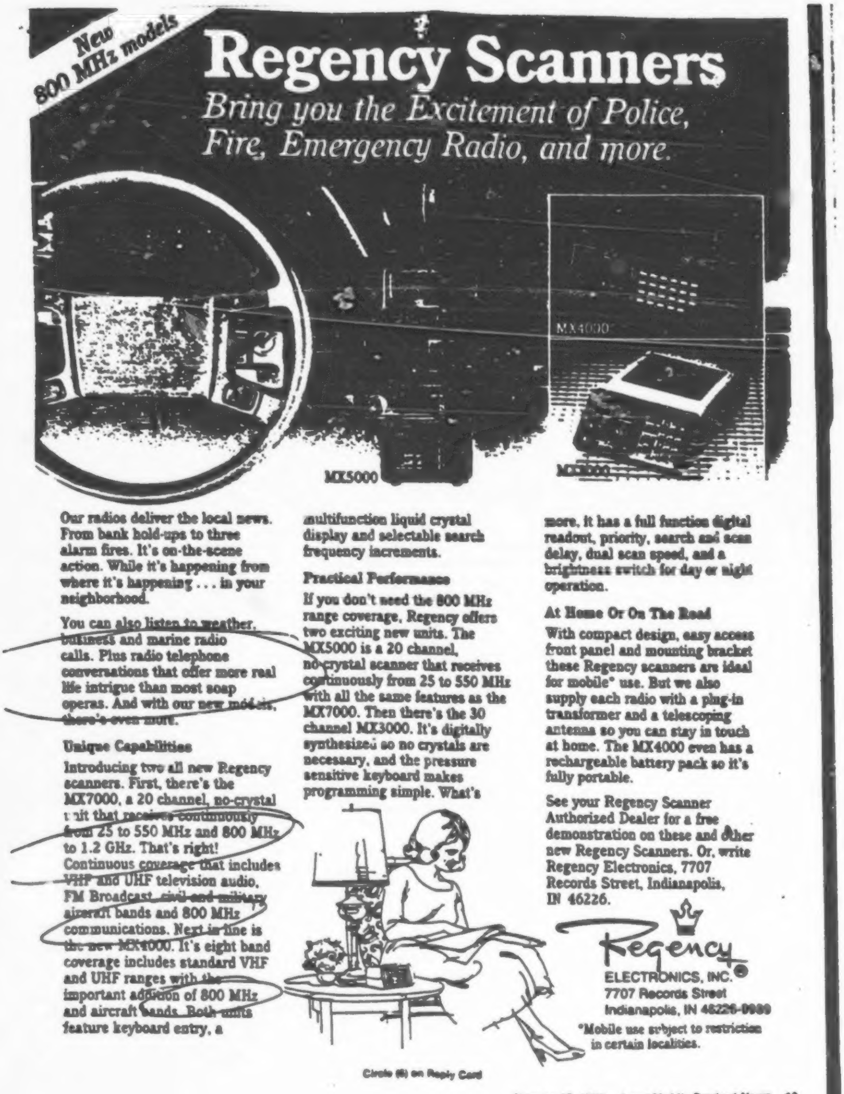
Thank you in advance for your cooperation in this request. It would be helpful to have a response within 10 business days. If you find that answering these questions requires additional time, please contact my staff (Deborah Leavy or David Beier at 225-3926).

Sincerely,

Bob Kastenmeier

ROBERT W. KASTENMEIER
Chairman
Subcommittee on Courts,
Civil Liberties and the
Administration of Justice

RWK:dlm


New 800 MHz models
MX4000
MX5000
MX3000

# Regency Scanners

*Bring you the Excitement of Police, Fire, Emergency Radio, and more.*

Our radios deliver the local news. From bank hold-ups to three alarm fires. It's on-the-scene action. While it's happening from where it's happening . . . in your neighborhood.

You can also listen to weather, business and marine radio calls. Plus radio telephone conversations that offer more real life intrigue than most soap operas. And with our new models, there's even more.

**Unique Capabilities**

Introducing two all new Regency scanners. First, there's the MX7000, a 20 channel, no-crystal unit that receives continuously from 25 to 550 MHz and 800 MHz to 1.2 GHz. That's right! Continuous coverage that includes VHF and UHF television audio, FM Broadcast, civil and military aircraft bands and 800 MHz communications. Next in line is the new MX4000. It's eight band coverage includes standard VHF and UHF ranges with the important addition of 800 MHz and aircraft bands. Both units feature keyboard entry, a multifunction liquid crystal display and selectable search frequency increments.

**Practical Performance**

If you don't need the 800 MHz range coverage, Regency offers two exciting new units. The MX5000 is a 20 channel, no-crystal scanner that receives continuously from 25 to 550 MHz with all the same features as the MX7000. Then there's the 30 channel MX3000. It's digitally synthesized so no crystals are necessary, and the pressure sensitive keyboard makes programming simple. What's more, it has a full function digital readout, priority, search and scan delay, dual scan speed, and a brightness switch for day or night operation.

**At Home Or On The Road**

With compact design, easy access front panel and mounting bracket these Regency scanners are ideal for mobile* use. But we also supply each radio with a plug-in transformer and a telescoping antenna so you can stay in touch at home. The MX4000 even has a rechargeable battery pack so it's fully portable.

See your Regency Scanner Authorized Dealer for a free demonstration on these and other new Regency Scanners. Or, write Regency Electronics, 7707 Records Street, Indianapolis, IN 46226.

Regency
ELECTRONICS, INC.®
7707 Records Street
Indianapolis, IN 46226-0989

*Mobile use subject to restriction in certain localities.

Circle (6) on Reply Card

January 15, 1985 *Land Mobile Product News* 13

# NEW! Lower Price Scanners

**Communications Electronics,™** the world's largest distributor of radio scanners, introduces new lower prices to celebrate our 15th anniversary.

## Regency‡ MX7000-CA

List price $699.95/CE **price $379.95/SPECIAL**
***10-Band, 20 Channel • Crystalless • AC/DC***
*Frequency range: 25-550 MHz. continuous coverage and 800 MHz. to 1.3 GHz. continuous coverage*

The *Regency* MX7000 scanner lets you monitor military, F.B.I., Space Satellites, Police and Fire Departments, Drug Enforcement Agencies, Defense Department, Aeronautical AM band, Aero Navigation Band, Fish & Game, Immigration, Paramedics, Amateur Radio, Justice Department, State Department, plus thousands of other radio frequencies most scanners can't pick up. The *Regency* MX7000 is the perfect scanner for intelligence agencies that need to monitor the new 800 MHz. cellular telephone band. The MX7000, now at a special price from CE.

## Regency® Z60-CA

List price $379.95/CE **price $179.95/SPECIAL**
***8-Band, 60 Channel • No-crystal scanner***
*Bands: 30-50, 88-108, 118-136, 144-174, 440-512 MHz.*
*Hear Police, Aircraft and the FM Broadcast Bands.*

The *Regency* Z60 covers all the public service bands plus aircraft and FM music for a total of eight bands. The Z60 also features an alarm clock and priority control as well as AC/DC operation. Order today.

## Regency® Z45-CA

List price $329.95/CE **price $159.95/SPECIAL**
***7-Band, 45 Channel • No-crystal scanner***
*Bands: 30-50, 118-136, 144-174, 440-512 MHz.*

The *Regency* Z45 is very similar to the Z60 model listed above however it does not have the commercial FM broadcast band. The Z45, now at a special price from Communications Electronics Inc.

## Regency® RH250B-CA

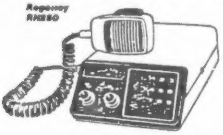
List price $613.00/CE **price $329.95/SPECIAL**
***10 Channel • 25 Watt Transceiver • Priority***

The *Regency* RH250B is a ten-channel VHF land mobile transceiver designed to cover any frequency between 150 to 162 MHz. Since this radio is synthesized, no expensive crystals are needed to store up to ten frequencies without battery backup. All radios come with CTCSS tone and scanning capabilities. A monitor and night/day switch is also standard. This transceiver even has a priority function. The RH250 makes an ideal radio for any police or fire department volunteer because of its low cost and high performance. A UHF version of the same radio called the RU150B covers 450-482 MHz. but the cost is $449.00. To get technician programming instructions, order a service manual from CE with your radio system.

## *NEW!* Bearcat® 50XL-CA

List price $199.95/CE **price $114.95/SPECIAL**
***10-Band, 10 Channel • Handheld scanner***
*Bands: 29.7-54, 136-174, 406-512 MHz.*

*The Uniden Bearcat* 50XL is an economical, hand-held scanner with 10 channels covering ten frequency bands. It features a keyboard lock switch to prevent accidental entry and more. Also order part # **BP50** which is a rechargeable battery pack for $14.95, a plug-in wall charger, part # **AD100** for $14.95 and also order optional cigarette lighter cable part # **PS001** for $14.95.



## *NEW!* JIL SX-400-CA

List price $799.95/CE **price $469.95/SPECIAL**
***Multi-Band, 20 Channel • No-crystal Scanner***
***Search • Lockout • Priority • AC/DC***
*Frequency range: 26-520 MHz. continuous coverage.*
*With optionally equipped RF converters 150KHz.-3.7 GHz.*

The JIL SX-400 synthesized scanner is designed for commercial and professional monitor users that demand features not found in ordinary scanners. The SX-400 will cover from 150 KHz. to 3.7 GHz. with RF converters. Order the following RF converters for your SX-400 scanner: **RF-1030-CA** at $234.95 each for frequency range 150 KHz. - 30 MHz. USB, LSB, CW and AM. (CW filter required for CW signal reception). **RF-5080-CA** at $194.95 each for 500-800 MHz. **RF-8014-CA** at $194.95 each for 800 MHz.-1.4 GHz. Be sure to also order **ACB-300-CA** at $99.95 each which is an antenna control box for connection of the RF converters. The **RC-4000-CA** data interface at $259.95 each gives you control of the SX-400 scanner and RF converters through a computer. Add $3.00 shipping for each RF converter, data interface or antenna control box. If you need further information on the JIL scanners, contact JIL directly at 213-926-6727 or write JIL at 17120 Edwards Road, Cerritos, California 90701 U.S.A.

## *SPECIAL!* JIL SX-200-CA

List price $499.95/CE **price $157.95/SPECIAL**
***Multi-Band - 16 Channel • No-Crystal Scanner***
*Frequency range: 26-88, 108-180, 380-514 MHz.*

The JIL SX-200 has selectable AM/FM receiver circuits, tri-switch squelch settings - signal, audio and signal & audio, outboard AC power supply - DC at 12 volts built-in, quartz clock - bright vacuum fluorescent blue readouts and dimmer, dual level search speeds, tri-level scan delay switches, 16 memory channels in two channels banks, receive fine tune (RIT) ± 2KHz., dual level RF gain settings - 20 db pad, AGC test points for optional signal strength meters all for this special price.

## Regency® HX1000-CA

List price $329.95/CE **price $189.95/SPECIAL**
***6-Band, 30 Channel • No Crystal scanner***
***Search • Lockout • Priority • Scan delay***
***Sidelit liquid crystal display • Digital Clock***
*Frequency range: 30-50, 144-174, 440-512 MHz.*

The new handheld *Regency* HX1000 scanner is fully keyboard programmable for the ultimate in versatility. You can scan up to 30 channels at the same time. The LCD display is even sidelit for night use. Order **MA-256-CA** rapid charge drop-in battery charger for $68.95 plus $3.00 shipping/handling. Includes wall charger, carrying case, belt clip, flexible antenna and nicad battery. Order now.

## *NEW!* Bearcat® 100XL-CA

List price $349.95/CE **price $209.95/SPECIAL**
***9-Band, 16 Channel • Priority • Scan Delay***
***Search • Limit • Hold • Lockout • AC/DC***
*Frequency range: 30-50, 118-174, 406-512 MHz.*

The world's first no-crystal handheld scanner now has a LCD channel display with backlight for low light use and aircraft band coverage at the same low price. Size is 1¾" x 7½" x 2¾." The *Bearcat* 100XL has wide frequency coverage that includes all public service bands (Low, High, UHF and "T" bands), the AM aircraft band, the 2-meter and 70 cm. amateur bands, *plus* military and federal government frequencies. Wow...what a scanner!

Included in our low CE price is a sturdy carrying case, earphone, battery charger/AC adapter, six AA ni-cad batteries and flexible antenna. Order your scanner now.

## *NEW!* Regency® HX1200-CA

***New direct channel access feature***
List price $369.95/CE **price $214.95/SPECIAL**
***8-Band, 45 Channel • No-crystal scanner***
***Priority control • Search/Scan • AC/DC***
***Sidelit liquid crystal display • EAROM Memory***
*Bands: 30-50, 118-136, 144-174, 406-420, 440-512 MHz.*

The new HX1200 scanner operates on 120V AC or 9.6 VDC. Permanent memory backup. Size 2¾" x 2" x 7¾." Includes wall charger, carrying case, belt clip, flexible antenna and nicad batteries. Order today.

## *SPECIAL!* Bearcat® DX1000-CA

List price $649.95/CE **price $339.95/SPECIAL**
*Frequency range 10 KHz. to 30 MHz.*

The *Bearcat* DX1000 shortwave radio makes tuning in London as easy as dialing a phone. Features PLL synthesized accuracy, two time zone 24-hour digital quartz clocks and more. Add $12.00 for shipping.

CIRCLE 172 ON READER SERVICE CARD

## *NEW!* Bearcat® 800XLT-CA

List price $499.95/CE **price $299.95/SPECIAL**
***12-Band, 40 Channel • No-crystal scanner***
***Priority control • Search/Scan • AC/DC***
*Bands: 29-54, 118-174, 406-512, 806-912 MHz.*

The Uniden 800XLT receives 40 channels in two banks. Scans 15 channels per second. Size 9¼" x 4½" x 12½."

### *OTHER RADIOS AND ACCESSORIES*

| | |
|---|---|
| Panasonic RF-2600-CA Shortwave receiver | $179.95 |
| Panasonic RF-B300-CA Shortwave receiver | $195.95 |
| RD95-CA Uniden Remote mount Radar Detector | $139.95 |
| RD55-CA Uniden Visor mount Radar Detector | $119.95 |
| BC 20/20-CA Bearcat 40 channel scanner SALE | $224.95 |
| BC 210XW-CA Bearcat 20 channel scanner SALE | $209.95 |
| BC 260-CA Bearcat 16 channel scanner SALE | $194.95 |
| BC 300-CA Bearcat 50 channel scanner SALE | $254.95 |
| BC-WA-CA Bearcat Weather Alert™ | $39.95 |
| DX1000-CA Bearcat shortwave receiver SALE | $339.95 |
| PC22-CA Uniden remote mount CB transceiver | $99.95 |
| PC55-CA Uniden mobile mount CB transceiver | $59.95 |
| Z45-CA Regency 45 channel scanner SALE | $159.95 |
| R1060-CA Regency 10 channel scanner | $98.95 |
| MX3000-CA Regency 30 channel scanner | $199.95 |
| XL156-CA Regency 10 channel scanner SALE | $129.95 |
| UC102-CA Regency VHF 2 chan. 1 Watt transceiver | $119.95 |
| RH250B-CA Regency 10 channel VHF transceiver | $329.95 |
| RU150B-CA Regency 10 channel UHF transceiver | $449.00 |
| RPH410-CA 10 ch. handheld no-crystal transceiver | $379.95 |
| BC10-CA Battery charger for Regency RPH410 | $79.95 |
| MA256-CA Drop-in charger for HX1000 scanner | $68.95 |
| MA257-CA Cigarette lighter cord for HX1000 | $19.95 |
| MA917-CA Ni-Cad battery pack for HX1000 | $29.95 |
| EC10-CA Programming tool for Regency RPH410 | $20.00 |
| SMRH250-CA Service man. for Regency RH250 | $20.00 |
| SMRU150-CA Service man. for Regency RU150 | $20.00 |
| SMRPH410-CA Service man. for Regency RPH410 | $20.00 |
| SMMX7000-CA Svc. man. for MX7000 & MX5000 | $20.00 |
| SMMX3000-CA Service man. for Regency MX3000 | $20.00 |
| B-4-CA 1.2 V AAA Ni-Cad batteries (set of four) | $9.00 |
| A-135C-CA Crystal certificate | $3.00 |
| FB-E-CA Frequency Directory for Eastern U.S.A. | $12.95 |
| FB-W-CA Frequency Directory for Western U.S.A. | $12.95 |
| TSG-CA "Top Secret" Registry of U.S. Govt. Freq. | $14.95 |
| TIC-CA Techniques for Intercepting Comm. | $14.95 |
| RRF-CA Railroad frequency directory | $10.00 |
| CIE-CA Covert Intelligenct, Elect. Eavesdropping | $14.95 |
| A60-CA Magnet mount mobile scanner antenna | $35.00 |
| A70-CA Base station scanner antenna | $35.00 |
| USAM06-CA Mag mount VHF/UHF ant. w/ 12' cable | $39.95 |
| USAK-CA ¾" hole mount VHF/UHF ant. w/ 17' cable | $35.00 |
| USATLM-CA Trunk lip mount VHF/UHF antenna | $35.00 |

Add $3.00 shipping for all accessories ordered at the same time.
Add $12.00 shipping per shortwave receiver.
Add $7.00 shipping per scanner and $3.00 per antenna.

### *BUY WITH CONFIDENCE*

To get the *fastest delivery from CE* of any scanner, send or phone your order directly to our Scanner Distribution Center™ Michigan residents please add 4% sales tax or supply your tax I.D. number. Written purchase orders are accepted from approved government agencies and most well rated firms at a 10% surcharge for net 10 billing. All sales are subject to availability, acceptance and verification. All sales on accessories are final. Prices, terms and specifications are subject to change without notice. All prices are in U.S. dollars. Out of stock items will be placed on backorder automatically unless CE is instructed differently. A $5.00 additional handling fee will be charged for all orders with a merchandise total under $50.00. Shipments are F.O.B. Ann Arbor, Michigan. No COD's. Most products that we sell have a manufacturer's warranty. Free copies of warranties on these products are available prior to purchase by writing to CE. Non-certified checks require bank clearance.

**Mail orders to:** Communications Electronics,™ Box 1045, Ann Arbor, Michigan 48106 U.S.A. Add $7.00 per scanner for U.P.S. ground shipping and handling in the continental U.S.A. For Canada, Puerto Rico, Hawaii, Alaska, or APO/FPO delivery, shipping charges are three times continental U.S. rates. If you have a Visa or Master Card, you may call and place a credit card order. Order toll-free in the U.S. Dial 800-USA-SCAN. In Canada, order toll-free by calling 800-221-3475. Telex CE anytime, dial 810-223-2422. If you are outside the U.S. or in Michigan dial 313-973-8888. Order today.

Scanner Distribution Center™ and CE logos are trademarks of Communications Electronics Inc.
† Bearcat is a registered trademark of Uniden Corporation.
‡ Regency is a registered trademark of Regency Electronics Inc.
AD #011586-CA

Copyright © 1986 Communications Electronics Inc.

**For credit card orders call**
**1-800-USA-SCAN**

COMMUNICATIONS ELECTRONICS INC.™

***Consumer Products Division***
P.O. Box 1045 □ Ann Arbor, Michigan 48106-1045 U.S.A.
Call 800-USA-SCAN or outside U.S.A. 313-973-8888

BEST COPY AVAILABLE

CBS
CBS Inc., 1800 M Street, N.W.
Suite 300 North
Washington, D.C. 20036
(202) 457-4501

Robert A. McConnell
Vice President
CBS Washington

Dear Chairman Kastenmeier: February 4, 1986

On January 30, 1986, Richard L. Brown, counsel to Satellite Television Association, Inc./SPACE, submitted written testimony to your Subcommittee on H.R. 3378, the "Electronic Communications Privacy Act of 1985." As part of this testimony, Mr. Brown urged that your Subcommittee amend Section 101(g)(iii)(II) of that bill.

Mr. Brown asserts that the intent of the proposed amendment is simply to make "clear that if viewing of particular satellite programming is lawful under the provisions of Section 705(a) or Section 705(b) of the Communications Act of 1934, it is not made unlawful by implication of the provisions of H.R. 3378." However, a review of the text of his testimony and accompanying letter to you dated January 28, 1986, makes it apparent that "SPACE" has an underlying objective which is much more substantive and controversial. In essence, that objective is to call into question the application of Section 705 to the unauthorized interception and use of network feeds carried by satellite.

These satellite feeds serve as a vital means of business communication between the networks and their affiliated stations. On a regular basis, the feeds provide local stations with a "package" of network programs and network television advertising. This package contains gaps which, prior to retransmission to broadcast audiences, are filled with local station commercials, public service announcements and promotional materials. In addition, during hours when network programming is not scheduled, the satellite feeds include such material as scheduling information, previews of up-coming broadcasts, discussions of current management, financial and regulatory issues, and unedited news and sports footage which is intended for inclusion in local newscasts. These transmissions are precisely the sort of private communications which Congress sought to protect when it enacted Section 705 and its predecessor (old Section 605).

However, through a tortured reading of the Communications Act and a mischaracterization of antiquated case law, Mr. Brown has attempted to raise doubts and confusion where none should exist. As detailed in the attached memorandum from former FCC Chairman Richard E. Wiley, now with the law firm of Wiley & Rein, and the letter to you from Jack D. Smith, General Counsel, Federal Communications Commission, dated November 27, 1985, the language of Section 705 as well as its legislative history and judicial interpretation make it quite clear that Congress intended the section to prohibit the signal "pirating" activities that Mr. Brown would like to encourage.

Protection against such piracy is a matter of great importance not only to networks and other program suppliers, but also to hundreds of local television stations across the country and the communities they are licensed to serve. Affiliated stations supplement the network feed with important services such as local news, weather, public affairs, sports and other local public service programming. Critical local information does not and cannot reach its intended audience when owners of backyard earth stations bypass the local affiliate by pirating the network's satellite feed. Interception of the network feed also creates disincentives for local broadcasters to increase their coverage areas by expanding their own facilities or supplementing service through the use of terrestrial "translators" that rebroadcast the local station's signal to underserved areas.

Moreover, it is a well-recognized fact that the economic health of these stations is dependent on the generation of advertising revenue which, in turn, is a function of the audience ratings that they achieve within their service areas. Individuals who view network programming by intercepting the satellite feed would not see the commercials that are inserted by the local stations prior to retransmission to their broadcast viewing audiences. Furthermore, such individuals would not be considered by the ratings services to be members of local station audiences. Accordingly, the diversion of viewers away from these stations, through widespread direct reception of the network satellite feed, would have severe adverse consequences for this country's system of locally-based television broadcasting.

We are hopeful that Congress will continue to be vigilant in maintaining clear-cut statutory protection against such unauthorized reception and use of satellite feeds. For this reason, we urge you to avoid taking any action, at the behest of "SPACE" or others, which would call into question the application of the existing Section 705 to these improper activities.

Should you desire any additional information concerning this important matter, please feel free to call me at any time.

Sincerely yours,

Robert A. McConnell

Robert A. McConnell

The Honorable Robert W. Kastenmeier, Chairman
Subcommittee on Courts, Civil Liberties
and the Administration of Justice
Committee on the Judiciary
United States House of Representatives
2137 Rayburn House Office Building
Washington, D.C. 20515

cc: Jack Smith, General Counsel, FCC
All Members of Subcommittee on Courts, Civil Liberties and the Administration of Justice

WILEY & REIN

## MEMORANDUM

We have examined two letters to the Honorable Robert W. Kastenmeier, Chairman of the House Subcommittee on Courts, Civil Liberties, and the Administration of Justice. The first of these letters, authored by Jack D. Smith, General Counsel of the Federal Communications Commission, finds that, pursuant to Section 705 of the Communications Act, unauthorized interception and viewing of network satellite feeds could subject the interceptor to civil and criminal penalties. The second letter, prepared by Richard L. Brown, counsel to the Satellite Television Industry Association/SPACE, attempts to show that Section 705 is inapplicable to the interception and viewing of these network feeds.

As detailed below, the views expressed by the FCC's General Counsel represent a correct reading of Section 705 of the Communications Act and are based on a sound understanding of the relevent statutory language and legislative history. In addition, the General Counsel's findings are fully in accord with the numerous judicial decisions that have dealt with the implementation of this provision and its predecessor.

In contrast, the letter put together by the counsel for "SPACE" represents a strained and wholly-ineffective effort to reach a pre-ordained conclusion. It ignores virtually all modern case law on the subject and relies instead on misleading, and highly selective, references to decisions which date back to the 1930's. Furthermore, to the extent that it deals with the legislative history of Section 705, it relies on fragments of the legislative debate which deal obliquely with the matter at hand, and ignores an authoritative Congressional pronouncement which makes clear that Section 705 applies to satellite feeds of programming that are intended for retransmission by local broadcast stations to the public at large.

## I. The Statutory Language

Section 705 contains four distinct provisions which are designed to deal with the unauthorized interception and utilization of radio communications.[1] These provisions are contained in the first four sentences of Subsection 705(a) and may be summarized as follows:

---

[1] Section 705 is codified by the editors of the United States Code Annotated as 47 U.S.C.A. § 605.

BEST COPY AVAILABLE

(1) persons employed by communications enterprises are prohibited from divulging the contents of transmissions except to authorized recipients.

(2) persons who are not authorized by the sender are prohibited from "intercept[ing]" radio communications and "divulg[ing] or publish[ing]" their contents to any person.

(3) persons who are not entitled thereto are prohibited from "receiv[ing]" any "interstate or foreign" communication and "us[ing]" the contents of such communication for their "own benefit or for the benefit of another not entitled thereto."

(4) persons who receive intercepted radio communications are prohibited from "divulg[ing]" or "us[ing]" their contents.

The FCC General Counsel's letter focuses on the third of these prohibitions. The counsel for "SPACE" argues that private individuals who intercept communications can be held liable, "if at all," only under the second of the prohibitions outlined above.

The final sentence of Subsection 705(a) provides that the prohibitions listed above are not applicable to radio communications which are transmitted by any station with the intent that they be "for the use of the general public."2/ This provision assures that the signals which broadcasters intend for use by the public may, in fact, be utilized for that purpose.

---

2/ In 1984, Congress adopted an additional exemption which, in certain circumstances, permits the receipt and use for private viewing of programming which is "primarily intended for direct receipt by cable operators for their retransmission to cable subscribers." 47 U.S.C.A. § 605(b) and (c). The General Counsel's letter correctly notes that this exemption is not applicable to network satellite feeds which are primarily intended for direct reception by conventional broadcast stations.

## II. The FCC General Counsel's Letter

The third sentence of Subsection 705(a), which was relied upon by the FCC General Counsel, reads as follows: "[n]o person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto." This provision applies to all interstate and foreign radio communications except those intended for "the use of the general public." Id.

As the General Counsel correctly notes, the networks' nationwide satellite feeds clearly constitute "interstate" radio communications.3/ Moreover, as recognized by the courts, the viewing of television signals by a homeowner plainly constitutes a use of this material "for his own benefit." See. e.g., Movie Systems, Inc. v. Heller, 710 F.2d 492 (8th Cir. 1983); Hoosier Home Theater, Inc. v. Adkins 595 F. Supp. 389 (S.D. Ind. 1984).

Thus, the principal remaining statutory question is whether the networks intend that their satellite feeds be transmitted for "the use of the general public." See Chartwell Communications Group v. Westbrook, 637 F.2d 459, 464-65 (6th Cir. 1980) (the critical factor is the intent of the party transmitting the radio communications). In this regard, the General Counsel was clearly correct in concluding that the networks intend that their satellite feeds be

---

3/ Both the House and Senate have explictly recognized that Section 705 prohibits not only unauthorized interception of traditional radio communications, but also communications transmitted by means of new technologies -- including satellite communications. See 130 Cong. Rec. H10493 (daily ed. Oct. 1, 1984); 130 Cong. Rec. S14287 (daily ed. Oct. 11, 1984). Indeed, the courts recognized the applicability of its predecessor Section 605 to such communications. See, e.g., Rainbow Programming Services v. Hirabbai R. Patel, No. PCA 82-6009 (N.D. Fla., November 8, 1982); National Football League v. American Embassy Inc., No. 83-0701 (S.D. Fla. March 25, 1983). Quite recently, the same result has been reached in judicial interpretation of the present Section 705. Pro Am Sports System, Inc. v. Larry Simone, Inc., Civil No. 84CV2032DT (E.D. Mich., January 15, 1986).

utilized solely by their affiliated stations. The raw satellite feed is transmitted with gaps to be filled in through the insertion of local advertising, public service announcements and promotional material prior to broadcast by affiliated stations to the general public. Since the networks and their affiliates depend on advertising as their main source of revenue (and advertising is a function of the size of the viewing audience), it is obvious that they have a powerful economic incentive to assure that this local material is inserted before making the programming available to the public. Indeed, CBS has recently taken steps to "scramble" its network satellite feed to assure that this objective is not defeated.4/

It is also significant that, during hours when the network is not programming, the satellite feed includes internal business communications such as scheduling information, discussion of current financial, management and regulatory issues, previews of upcoming features, advanced delivery of promotional material and unedited news and sports footage. The inclusion of this material in the satellite feed underscores the fact that the transmissions are intended solely for the use of CBS affiliated stations -- not the general public.5/

Thus, it is apparent that the General Counsel's letter rests on an accurate understanding of the character of network satellite feeds and a correct reading of the law.

## III. The Letter Prepared by the Counsel for "SPACE"

The counsel for "SPACE" advances several arguments in an effort to rebut the findings reached by the FCC's General Counsel.

---

4/ As the General Counsel's letter correctly notes, "[e]xisting case precedent does not require . . . that networks scramble their signals in order to be encompassed within Section 705." See Movie Systems, Inc. v. Heller, supra at 495 n. 7., Home Box Office, Inc. v. Advanced Consumer Technology, Movie Antenna, Inc. 549 F. Supp. 14, 21-22 (S.D.N.Y. 1981); Hoosier Home Theatre, Inc. v. Adkins, supra at 396.

5/ Moreover, as noted in the General Counsel's letter, satellite transmissions are common carrier service on common carrier frequencies.

"SPACE" first attempts to show that the third sentence of Subsection 705(a) (which was relied upon by the FCC) is applicable only to the interception of signals by "persons employed in communications enterprises" -- and not to interceptions by individuals generally. This argument is both erroneous and irrelevant.

The argument is founded on "SPACE"'s incorrect assertion that the Supreme Court has "held" the third statutory prohibition to be applicable only to the receipt and unauthorized use of transmissions by the employees of communications enterprises. The case relied upon in this argument is Weiss v. United States, 308 U.S. 321 (1939). The Weiss case was decided under the second "clause" of old Section 605 which (like the second sentence of its successor, the current Section 705(a)) prohibited the unauthorized interception and divulgence of "interstate and foreign" communications.6/ The question before the Court was whether this particular provision extended to intrastate as well as interstate transmissions. The Court held that the second clause applied to both forms of transmission and, accordingly, that messages uncovered during illegal wiretaps of intrastate phone calls could not be divulged in court.

The Weiss Court's brief reference to clause three (which "SPACE" incorrectly characterizes as a "holding") was simply a recital of arguments that had been presented by the petitioners. The Court did not adopt these views as its own and, indeed, such a finding would have been unnecessary and inappropriate given the facts involved in the case.7/

Significantly, the letter prepared for "SPACE" entirely ignores a large body of modern case law which applies the third provision of Section 705 (the one discussed in the FCC General Counsel's letter) to interceptions by individuals who were not employees of communications enterprises. These cases include:

---

6/ Under old Section 605, the four basic prohibitions on unauthorized interceptions were divided into clauses rather than sentences which is the format utilized in the current Section 705.

7/ "SPACE" also relied upon another 1930's case (Sablowsky v. United States, 101 F.2d 183 (3rd Cir. 1938)) in an effort to bolster its argument. While Sablowsky does contain dicta along the lines suggested by "SPACE", the holding, like that in Weiss, dealt with the question of whether wiretaps of intrastate communications could be used as evidence in court. In any event, the dicta in Sablonsky has been uniformly ignored (and, as a practical matter, rejected) in modern jurisprudence.

- -- Subscription Television of Greater Washington v. Kaufmann, 606 F. Supp. 1540 (D.C. D.C. 1985) (defendant sold decoders to the public to permit unscrambling of STV signals).

- -- Chartwell Communications Group v. Westerbrook, supra, (defendants sold electronic decoders to the public to facilitate unauthorized interception of an STV signal.)

- -- Hoosier Home Theater, Inc. v. Adkins, supra, (defendant homeowner was engaged in unauthorized interception and use of a microwave television signal).

- -- Home Box Office, Inc. v. Advanced Consumer Technology, Movie Antenna, Inc., supra, (defendants were a manufacturer and a distributor who sold equipment which allowed members of the general public to intercept and view microwave television signals).

- -- Movie Systems, Inc. v. Heller, supra, (defendant was a private individual who installed equipment to receive and view microwave television programming.)

Furthermore, even if "SPACE" were correct in asserting that the third provision is applicable only to communications industry employees, its argument would be irrelevant to the underlying objective that "SPACE" is endeavoring to advance. This is true because, in any event, unauthorized interception and home viewing of network satellite feeds would violate the second clause of Section 705. As previously noted, that clause (which "SPACE" concedes is applicable to "any person") forbids the unauthorized interception and divulgence of communications. While "SPACE" argues that home viewing does not constitute divulgence within the meaning of this clause, the courts have already held to the contrary.

The second provision states that "[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communications to any person." 47 U.S.C.A. § 605. In National Subscription Television v. S&H TV, 644 F.2d 820, 827 (9th Cir. 1981), the court found that "the act of viewing" unauthorized television programming constituted "divulgement or publication." In addition, it determined that the unauthorized viewing of intercepted television programming "amounts to disclosure of the existence, contents, substance, purport, effect or meaning of" the transmitted signal. Id. Accord California Satellite Systems v. Seimon, 767 F.2d 1364 (9th Cir. 1985). Thus, even if the "holding" in Weiss were as suggested by "SPACE," it would make no difference in the dispute at issue here.

"SPACE" also argues that the network satellite feeds are intended for reception by the general public but, as noted above, this assertion is entirely without merit. Indeed, any question of the intent of CBS should be firmly put to rest by the network's action in scrambling its feed transmissions -- for the express purpose of preventing unauthorized public reception.

Finally, "SPACE" cites isolated segments of legislative history in an effort to imply the existence of some support for its position. In so doing, it wholly ignores the Comments of Senate Commerce Committee Chairman Robert Packwood which are directly on point. In discussing the adoption of a narrow statutory exemption for individual reception of "satellite cable programming," Senator Packwood stated that the exemption

> does not apply to feeds of programming or program material carried by satellite that are intended for internal use or for broadcast stations for retransmission to the public at large. Such program material remains subject to section 705 . . . .

130 Cong. Rec. S14283 (daily ed. Oct. 11, 1984) (Statement of Senator Packwood). Indeed, if Section 705 were not applicable to such interceptions and viewing activities generally, it is difficult to imagine why Congress would have had any interest in adopting the exemption for such viewing of "satellite cable programming," which is discussed at footnote 2, supra.

* * *

Accordingly, it is apparent that the views expressed in the letter of the FCC's General Counsel are correct.

WILEY & REIN

By Richard E. Wiley
Richard E. Wiley

February 4, 1986

# TESTIMONY OF RICHARD L. BROWN BEFORE THE SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE OF THE COMMITTEE ON THE JUDICIARY, UNITED STATES HOUSE OF REPRESENTATIVES

January 30, 1986

Mr. Chairman and Members of the Subcommittee. My name is Richard Brown, and I am representing Regency Electronics, Inc. ("Regency") with respect to its comments regarding H.R. 3378, a bill to amend the provisions of Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Act"), relating to interception of private communications through "wiretapping" and "eavesdropping." 18 U.S.C. Section 2510 et seq.

H.R. 3378 attempts to protect the privacy of communications, with certain exceptions, which embody messages transmitted via a "wire, radio, electromagnetic or photoelectric system that effects interstate or foreign commerce."

## I. Introduction and Summary

Regency is an Indiana-based communications manufacturing concern with over 1,500 employees in locations in Florida, Kansas, Nevada, New York and Nebraska. Amongst other electronic communications equipment, Regency manufactures radio band scanners — which are receive-only devices which scan the radio spectrum from 25 MHz through 1.3 GHz and receive all radio communications transmitted via those frequencies. Regency manufactures scanners both for amateur hobbyists' use and professional operations. The public benefits resulting from scanner use have long been acknowledged and applauded. In many rural areas of the country scanners provide unique public safety services to Americans who are isolated from traditional means of receiving news and information. Today there are over ten million scanners in use throughout the country.

Together with Uniden Corporation of America, Regency produces a substantial majority of the scanners currently marketed in America. These two companies have similar views and are both providing testimony urging the Congress not to pass legislation restricting reception rights. Reception of radio signals has been a cherished, fundamental American right since the inception of radio communications.

Regency wholeheartedly supports the Subcommittee's efforts to clarify the rights and expectations of personal and business users of new communications technologies under the Omnibus Act relating to privacy in communications. The advent of new technology has made it increasingly obvious that the public needs to be made aware of those communications devices which have an expectation of privacy and those which do not. Since the inception of federal regulation of the airwaves, Congress and the Federal Communications Commission ("FCC") have acknowledged the public's right to receive unencrypted radio communication. As a matter of public policy, Regency suggests that the Congress should not abrogate the public's right to receive unencrypted radio signals which are readily available to the American public.

### II. The Definition of Terms and Phrases in the Legislation Should Be Clarified to Exclude the Simple Monitoring of Radio Communication

The phrase "communication readily accessible to the public" is not defined in H.R. 3378 and its interpretation could result in serious liability, including criminal penalties, for millions of Americans who currently engage in the monitoring of unencrypted radio communications.

H.R. 3378 seeks to ensure the privacy of some electronic communications and Section 101(b) provides that it shall not be unlawful for any person to "intercept any electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public." On its face, this language can be read to permit the interception of any unencrypted electronic communication which can be received with a typical consumer electronics product, commonly available to Americans nationwide. But because of the absence of a specific definition, the intended exclusion might actually be read to prohibit consumers from receiving any or some type of unencrypted radio communication. Additionally, the term "intercept" is likely to be construed to attach serious liability to the mere receipt of communication without "divulgence." This is a substantial deviation from the Communications Act where liability for receipt of non-encrypted signals requires not only "interception" but also "divulgence" of the contents. This could be cured by the substitution of "interception" with "interception and divulgence" or alternatively the inclusion of an exemption for those who solely monitor radio communication.

### III. Public Policy Has Developed a Long-Standing Right to Receive Unencrypted Radio Communication

Since Congress passed the Radio Act of 1912, the American public has enjoyed the right to receive radio communication, without limitation. The Congress, through federal communications legislation, has vested this right in the American public — it is a right which the public expects and a right upon which the public relies. Not only would the proposed legislation clash with the present Communications Act (47 U.S.C. 101 et seq.) but it would overturn Congressional policy which has supported the public "right to listen" since the inception of federal radio regulation.

In 1912, S. 6412, as reported by Committee, provided that "every operator shall preserve the secrecy of radiograms." At the hearings on the bill Charles Stewart, an amateur operator and chairman of the Legislative Committee of the Wireless Association, explained that amateurs overhear messages on the airwaves but do not appropriate or use them. Congress agreed to include a provision in the bill which penalized divulgence, but permitted reception. This policy has been followed by the Congress ever since.

There is not presently any evidence to support a complete turnaround on this long-standing policy. Indeed, as recently as the 1984 Cable Communications Policy Act (which added Section 705(b) to the Communications Act), the Congress reaffirrmed its long-standing position that if electronic signals are unencrypted, the American public has a right to receive them. To the extent that H.R. 3378 operates to penalize mere interception of any non-encrypted radio signals, it is inconsistent with long-standing communications policy.

As a matter of policy this right should not be impeded by federal legislation, particularly where there is no substantial and compelling public need. It appears that the right to receive unencrypted radio communications is now being challenged by some cellular telephone interests which seek to persuade Congress to institute legislation prohibiting the public receipt of communications on frequencies which carry cellular radio communications. Cellular telephone support for such legislation is apparently based on the desire to affirm past representations and to ensure future representations to customers that cellular communications are secure and not subject to reception by the general public. For the reasons set forth below Regency opposes any restrictions on the public's right to receive any unencrypted radio communications and, in particular, it opposes any restriction on the right to receive communications on the frequencies utilized by cellular radio technology.

## IV. Cellular Radio Licenses Have Never Had Any Expectation of Privacy

Cellular radio licensees and users have had absolutely no legitimate expectation of privacy for cellular radio communications. Cellular licensees were aware that cellular radio conversations were not secure when they received their licenses from the FCC. Cellular radio telephone communications are transmitted via the RF spectrum and in that regard are no different than any other omni-directional communication transmitted over the radio spectrum. Cellular telephone licensees have never had any reason to believe that such communication would be secured by the FCC's Regulations or by Congressional legislation. It is submitted that any user expectancy of privacy could have only come from misleading promotions.

The expectation of privacy in the use of wireline telephone technology is comparable to the public's right to expect privacy in the delivery of mail and Regency supports this right. It has developed as a fundamental right in the American way of life. But if a wireline telephone conversation is akin to mailing a letter, then a cellular conversation is akin to mailing a postcard. There is no expectation of privacy. The fabric of American society is not grounded in the expectation of privacy for car telephone conversations or indeed for a wide variety of radio conversations. Just as a mail carrier is not engaging in a criminal act when reading a third party postcard, neither should a consumer be liable for listening to the postcard of the telephone industry: the cellular radio telephone conversation. If the postcard sender wishes security, he is responsible to take his own precautions — likewise with the cellular radio telephone user. The precautions should not rest on the shoulders of the federal government and be supported by the unprecedented abrogation of the public's right to listen. There are literally millions of daily conversations on the radio spectrum in America. For decades land mobile radio services in the U.S. has adequately served millions of users who have never experienced "privacy" in communications, nor have they ever expected it. Any deviation for one class of service has the potential for creating a demand for far-reaching ad hoc changes in the communications structure of our country.

## V. Cellular Operators, Not the Public, Should Bear the Burden of Securing Cellular Conversations

If cellular telephone licensees or their customers wish to secure their communications, then the burden to do so should be on them and not on the American public. A number of companies are now engaged in developing encryption technology for cellular telephone systems, in addition to the companies identified in the Appendix to this testimony, which have already developed and are currently marketing cellular telephone voice scrambling devices. Such devices secure cellular telephone communication for those who wish to use them. Just as Congress in its deliberation of the Cable Communications Policy Act determined that a satellite programmer should encrypt its signal if it wished to secure its reception, so Congress should adopt the same position regarding cellular telephone communication. Such a position would be consistent with Congressional policy.

In addition to the substantial precedent which mandates against infringing on the public right to receive radio communications, there is no demonstrable reason to make an exception in Congressional policy solely to accommodate cellular telephone services.

## VI. Receipt of Any Particular Cellular Conversation is Difficult

Receipt of any particular cellular conversation is difficult because of the technology. Unlike conventional mobile telephone service, cellular permits the caller to dial directly, without the assistance of the traditional mobile telephone operator. Cellular telephones also have the exclusive use of frequencies — the communication cannot be accessed by another person with a cellular telephone (except for the person who is being called.)

Other factors render particular cellular conversations inherently more problematic to intercept. The transmit and receive frequencies used to complete a cellular call are not identical. This diminishes the opportunity of receiving a complete conversation unless the listener can randomly locate and receive both the transmit and receive channels. But perhaps, most importantly, the frequencies used in a cellular call are changing constantly as the user moves from cell to cell. This phenomenon of frequency change, called "hand-off," acts as a natural scrambling function to make following any particular cellular conversation exceedingly more difficult than for other radio communications. The imposition of federal legislation which commences the process of abrogating long-standing public rights is not justified in order to protect the privacy of cellular communication when the technical receipt of any particular cellular communication is already difficult.

### VII. The Public Interest Concerning the Privacy of Cellular Communications is Best Protected By Full Disclosure

There is no compelling evidence which would justify singling out cellular telephone communications as entitled to Congressional mandated security when all other spectrum users are responsible for securing their own communications. For example, cordless telephones, which act like mini-cellular systems, have been on the market for many years and have never been subjected to any expectation of privacy. Like cordless telephone users, cellular telephone users have no expectation of privacy and to the extent that the American public has been informed otherwise, it appears that requiring public disclosure is a more appropriate manner to protect the public interest. In fact, the FCC is exploring just such a disclosure requirement on a very similar issue, that of the susceptibility of cordless telephones to unauthorized billing.

In its Second Report and Order, released June 5, 1985, looking to new interim provisions for cordless telephones, the FCC proposed a labeling requirement whereby the consumer would be informed of the security features possessed by the cordless telephone he/she plans to purchase. The proposed requirement calls for the box or other package in which the cordless telephone is marketed to carry a statement in a prominent location which reads as follows:

> CAUTION The base unit in this cordless telephone may respond to other nearby units or radio noise resulting in telephone calls being dialed through this unit without your knowledge and possibly calls being misbilled. In order to protect against such occurrences, this cordless telephone is provided with the following features:

Report and Order, supra, at ¶4.

This labeling has been suggested in order to make certain that the public is aware of the susceptibility of cordless telephones to misbilling and the provisions which the manufacturer had taken to secure the unit. Similar public disclosure concerning the security of the communications accomplished via cellular telephones as well as the steps the manufacturer or operator has taken to secure the communications and a general description of what security measures the user can take would be appropriate.

In the FCC proceeding exploring securing cordless telephones from false billing, the FCC found that it was "preferable to allow the consumer to decide the degree of security protection he requires and cost he is willing to pay rather than prescribing minimal design requirements with cordless telephone security systems, which would provide insufficient security in high density urban environments and unneeded security in low density rural environments." Supra at ¶3. In addition, the FCC was concerned that consumers might be mislead into believing that they were buying a telephone that was immune to security problems because it met FCC standards when, in fact, the minimal security obtained would not have alleviated security problems in many circumstances. The issues surrounding the security situation of communications via cellular telephones is identical.

## VIII. It is Impractical to Protect Cellular Communications Through Federal Privacy Legislation

Securing cellular communications by federal legislation prohibiting its interception is impractical and will not guarantee even a minimal measure of privacy. Currently, Americans utilize millions of radio spectrum scanners which are capable of monitoring cellular telephone communications. Additionally, there are millions of other common electronic receivers already in the hands of the American public which are capable of receiving cellular and cordless telephone communications.

For example, a number of UHF television receivers are capable of receiving UHF Channels 72-84 which have been reallocated for cellular telephone use. This is particularly true of older television receivers which commonly featured continuous UHF tuning. In other words, millions of Americans can tune to the cellular radio band simply by using their television sets. Additionally, most standard AM band radio receivers can receive cordless telephones communications because frequencies utilized by a number of cordless telephone units are at the upper most end of the AM broadcast band.

Still other realities of modern two-way radio system operation makes the prohibition on receiving cellular communications impractical. FCC regulations require the monitoring of most two-way radio systems by system operators and users. Because cellular telephones and conventional two-way radio systems are frequently interconnected to one another (or "patched together"), particularly for business purposes, an operator or user monitoring a two-way radio channel could routinely become privy to a cellular telephone communication that is interconnected through a two-way radio system.

The potential for interception of cellular radio communication in all of the above instances is enormous.

For example:

1. A cellular telephone subscriber places a call to the office of a business associate. The receptionist tells him that his business associate, Tom, is in his car which is equipped with a radio and that they will "patch" the cellular telephone call through. Tom's company has a two-way radio system licensed in one of the private radio services and is authorized to interconnect with the telephone network. FCC regulations mandate that other parties sharing Tom's radio channel must monitor before transmitting so as to not cause interference to an ongoing transmission. Any portion of the cellular telephone communication is subject to interception by any other two-way radio licensee who is monitoring Tom's two-way frequency before beginning a transmission.

2. A consumer owns an older television set with continuous UHF tuning. In other words, the consumer can tune to the cellular band with her television set. While

searching for a channel she receives a cellular conversation. A friend who was also present thinks this is most interesting and later tells others about it. Word eventually gets to an individual who reports the consumer to the authorities. The consumer's only comfort is that there are at least several million other citizens who have the same potentiality of intercepting a cellular communication.

3. A typical American family is in the kitchen having dinner. Mom is tuning in some easy listening music at the high end of the AM band. Mom comes across a voice conversation and recognizes the voice as the next door neighbor with whom the family is not on very good terms. Apparently the neighbor has a cordless telephone which operates within the range of an AM radio. The next day the family's ten year old, who is on better terms with the neighbor's ten year old son, spills the beans about overhearing the conversation. The family has all but forgotten about the incident when it is served a subpoena. Here again, there are millions of citizens who will become at risk if the proposed legislation is not clarified.

Utilizing federal legislation to prohibit tens of millions of people from receiving communications with devices that are already in the hands of the American consumer is impractical. It places a tremendous burden on the government to protect privacy rights that have never before been recognized and which the framers of the Constitution could not have considered as protected speech. It sets an unworkable precedent of legislating news rights which, practically speaking, cannot be protected.

## IX. Protecting Specific Radio Frequencies is Imprudent

Protecting specific frequencies, such as the current cellular spectrum, is imprudent because of the spectrum allocation procedure. Although today cellular radio operates at specified frequencies in the 800 MHz-900 MHz band, different or additional frequency ranges may accommodate cellular radio communications in years to come.

The shifting of radio spectrum to different uses as technology develops and the need for certain types of radio services expands or shrinks, dictates against instituting legislation which is frequency specific. What was once reserved for UHF television spectrum is now used for cellular radio communications. Perhaps future allocations for cellular communications will come from radio spectrum now allocated to a service for which millions of Americans already have receivers. What is frequency specific privacy legislation at this time could result in chaos as a result of future spectrum allocation proceedings.

## X. Encryption is the Best Assurance of Privacy For Cellular Communication and Serves the Public Interest

Encryption systems are currently available for cellular communications and they provide the most practical and least burdensome means of securing cellular communications. The technology is there and it should be up to the cellular licensees and manufacturers to make it available to the public. Consumer demand will dictate a decrease in price and proliferation of options and features for cellular security technology. But such consumer demand will not develop if consumers are led to believe that federal legislation will ensure the privacy of cellular radio conversations.

The Congress has previously recognized the most practical alternatives to easily intercepted communication is provided by encryption technology. The 1985 Electronic Surveillance and Civil Liberties Report of the Office of Technology addressed the issue of safeguarding electronic communication.

> ...Satellite communication systems and digital switching and transmission technology are becoming pervasive, along with other easily intercepted technical applications such as cellular mobile radio, cordless telephones, electronic mail, computer conferencing and electronic bulletin boards... (Page 9).

The report concluded that the only technological countermeasure at this time that is thought to be generally effective, is encryption. What legislation cannot assure the

American public, technology can and encryption is the only reliable means for ensuring privacy of cellular communications.

### XI. Legislation Mandating Privacy Should Not Be Extended to Any Other Specific Radio Service

Comments provided previously to Congress on the issue of electronic privacy by other participants have encouraged the adoption of legislation safeguarding the privacy of marine telephone radio communications. The same policies which dictate against the adoption of specific privacy legislation for cellular communications also dictate against the adoption of privacy legislation regarding marine telephone communications. As a practical matter, marine telephone communications are identical to any type of conventional two-way radio communication. They are even more accessible to the public than cellular communications, as any craft equipped with a marine radio system can receive the communication of any other marine radio telephone user. Additionally, ready access to marine radio telephone communications by all craft operators, provides a valuable safety warning system which can be crucial in marine emergencies.

### XII. Clarification of the Definitions in the Legislation is Necessary

The bill provides penalties for simple interception and the meaning of "interception" as used in the legislation is ambiguous. Simple interception without divulgence or use of the information intercepted is a benign act. It can have no consequences. The Congress has never before adopted an approach where simple receipt of non-encrypted radio communications is prohibited. Its position has always been that interception and some type of divulgence is necessary. There is no crucial aspect to this situation which would support a deviation from this policy with the imposition of harsh penalties for simple reception of radio communications without divulgence of the communication.

It has never been established that the sender of a communication can claim a property right in the electronic signal itself. At this time it does not appear to be Congress' intent to extend unprecedented property rights in electronic impulses to cellular radio users. Clarifying the rights of the sender, as they relate to the right of the general public to receive communication, dictates an exclusion for the simple receipt of an electronic signal with the discretion to apply a penalty for divulging or using the information content of the signal. By adopting an exclusion for the simple monitoring of radio communications Congress would avoid the unintentional attachment of property rights to electronic impulses.

The bill does not discuss the monitoring of signals, but relies solely on interception as its definitional basis for prohibited behavior. The line between content divulgence or use versus simple receipt or monitoring of electronic impulses must be drawn. There is a distinct difference and Congress should support the continuence of Americans' rights to monitor unencrypted radio frequencies as well as the imposition of penalties for divulgence or misuse of information received from monitored communications.

It is submitted that the definition of "communication readily accessible to the public" be defined as any unencrypted radio communication. This will remove any questions concerning the public's long-standing right to continue to monitor unencrypted radio signals.

## XIII. Conclusion

For nearly 75 years the Congress and the FCC have staunchly defended the right of the American public to receive radio communications. It has been the touchstone of an open society, a characteristic unique to free and democratic countries. The "right to receive" has long been vested in the American public and it is a right upon which the public relies. As a matter of policy, we submit that Congress should oppose the adoption of any federal legislation which would abridge the public's right to receive radio communication.

Specifically regarding cellular communications, there is no logical reason to carve out an exemption to the long-standing policy of permitting reception of unencrypted radio signals. Cellular radio licensees and users have had no expectation of privacy and to the extent that the public is confused over whether or not cellular communications are secure, a full disclosure requirement in the labeling of cellular products would best serve the public interst.

If security in cellular communications is desired by the public, then encryption is the best alternative. First, it is the only measure which is workable and upon which the public can reasonably rely. Secondly, it is the cellular industry and its customers, not the American public, which should bear the burden of securing cellular communications — especially in this instance where the communication is easily accessible by millions of Americans, where its receipt is, in fact, a long-standing public right and where the technological means of securing the communications is available. To abridge the rights of millions of Americans to receive non-encrypted radio communications is the most restrictive, rather than the least restrictive alternative. Rather than the draconian meausre of criminalizing use of equipment in the hands of tens of millions of Americans, the least intrusive alternative would be to encourage the use of encoding equipment by those who desire it.

Regency would support adoption of the proposed legislation to the extent that the definition of communicatoin "readily accessible to the public" is clarified to include any unencrypted communication and to the extent that "intercepton" is defined as "receipt and divulgence" or excludes specifically simple monitoring of radio communication. These clarifications would be consistent with the policy and precedent of both the FCC and Congress and would thereby serve the public interest.

Thank you for this opportunity to provide testimony.

Respectfully submitted,

**REGENCY CORPORATION**

By: ______________________
Richard L. Brown

## APPENDIX

The following companies manufacture voice scramblers for use with cellular radio technology.

**Teltron Systems** 703-533-8555
Republic Group, 5801 Lee Highway, Arlington, VA 22207

- Model: SP-602 cellular voice scrambler

  This unit works on a speech inverter principle in a random sequence rendering the communication unintelligible to the casual listener.

- Model: TDM-16 2 dimensional encryption

  This is a more sophisticated unit which scrambles the communication making it totally secure in tactical real time.

- Model: TVC 9000 encryption system

  This provides the highest level government to government security and can handle world cellular communication.

Prices for Teltron security units begin in the $800 range.

**Transcrypt/International, Inc.** 800-228-0226
1440 Buckingham, Lincoln, NE 68506

- Model: SC-200

  This is a voice inversion unit. The prices for this unit is in the $250 range.

**Midien Electronics** 602-884-7981
2302 E. 22nd Street, Tuscon, AZ

- Model: VPU 1

  This is a cellular full duplex voice inversion model.

- Model: VPU 2

  This is a simplex voice inversion model.

The price for these units begins in the $125 range.

**AT&T** provides a cordless telephone (Model 8500) which has full scrambling capability. The cost of the unit is in the $250 range. AT&T also has available its line of AUTOPLEX Cellular Privacy/Data Products (promotional literature attached).

**Controlonics Corp.** (Unex Div) 617-692-3000/800-233-8639
5 Liberty Way, Westford, MA 01937

Model: FDS 301

This is a cellular voice scrambler which is frequency domain swept 33 codes. It also features selection of up to eight different code sequences. The price for this unit begins in the $600 range.

CRC 703-893-2880
8619 Westwood Center Drive, Vienna VA 22180

CRC is developing a totally secure cellular system which it expects to have ready within one year. All calls originated or received within the entire system will be secure. Such a system will provide greater security than currently exists for calls placed through the conventional existing wireline telephone system.

# AUTOPLEX™ Cellular Privacy/Data Product

### *Responding to Your Customers' Needs*

Development of the AUTOPLEX System Privacy/Data Product is based on the increasing number of current and future business, military and government cellular phone users openly concerned about the total privacy of their phone conversations and the security of data transmitted through the airwaves.

Offered on a system-wide or per customer basis, this AUTOPLEX System service makes use of Switch Resident Equipment (SRE), an AT&T Information Systems CTS 1620 Privacy/Data Accessory, and Key Modules. It offers three types of calls — mobile-to-land, land-to-mobile and mobile-to-mobile — plus a wide selection of customer features.

Both privacy and data applications will appeal to all levels of executives, government officials, professionals, military personnel, sales and service representatives plus all other cellular phone users wishing to protect their conversations.

The data security application can be used to access remote databases, such as stock market information, insurance databases, or order and inventory databases. No special equipment is needed at the destination being accessed, a definite competitive advantage.

### *Voice Privacy Benefits*

For service providers, Voice Privacy can allow current customers to discuss sensitive issues thereby increasing air time. It can also provide you with service differentiation to attract new corporate and government customers. The premium charge billed can generate increased system revenues. For customers, there is an increased level of privacy plus the capability to call any destination — privately — without the need for destination apparatus.

### *Data Security Benefits*

Service providers can take advantage of service differentiation, additional air time for data calls, premium billing and the opportunity to interest new users with specific data applications, e.g. field sales or service, order entry, stock checking and electronic mail.

Customers equipped with their own data terminals can receive data transmissions in their vehicles; protect access codes, passwords and sensitive information; call anywhere without special destination equipment; avoid hand-off and fading problems through error-free transmission; and save time using data speeds of 300/1200/2400 BPS.

### *System Configuration*

**Switch Resident Equipment (SRE):** The SRE consists of System Channel Units (SCUs), Data Sets and a Common Control Processor. Connected to trunks in an AUTOPLEX Mobile Telephone Switching Office, SCUs are compatible with four-wire E&M Type I and II trunks. The SRE responds to requests for private voice and data services activated through signaling tones and interfaces with trunk and signaling circuits. For data service, SCUs provide the capability to communicate with computer modems.

An optional Common Control Processor (required for systems with more than 48 System Channel Units) consists of terminals, two key processors and two operations processors. This equipment provides for secure dial back, remote equipment testing, SCU software download, class-of-service record, encryption-key usage records and administration of up to 500,000 encryption keys.

**CTS 1620 Accessory:** This unit is placed in a cellular phone user's trunk or passenger compartment and is connected to a cellular phone at the standardized interface between the control unit and transceiver unit. It communicates with the cellular phone and encrypts digitized voice signals to provide private voice service. Asynchronous data signals are also encrypted to provide data service. Both services use a Proprietary Digial Encryption Protocol.

**Key Modules:** Two modules containing encryption keys can be used. The fixed key module contains an encryption record used between the CTS 1620 and the SRE for privacy and data. The configuration/key module can hold a private encryption record used for end-to-end privacy and data.

AT&T

### *Features and Functions*

The AUTOPLEX Privacy/Data Product, when used with the CTS 1620, offers subscribers the following high performance features and functions:

**CTS 1620 Configuration Options:** The customer can select clear voice, private voice or data as the default service. The customer can also specify whether to enable or disable the blinking IN USE indicator on the cellular phone control unit and the phone dial code features. Data options such as automatic answer, data speed, full/half duplex, XON/XOFF flow control, stop bits, data bits and parity can also be specified.

**User Friendly Interface:** The CTS includes push buttons and status indicators for functions such as clear-voice service (CLR) and key/testing (K/T), cellular phone dial codes, control unit IN USE indicator, configuration and key interface, configuration and key module and DTE interface (RS-232).

**Additional Features:** This group of features includes updating CTS 1620 encryption keys, requesting CTS 1620 self-tests and reducing power consumption when there is no call in progress by automatically turning off the CTS 1620's processor power.

### *The Bottom Line: Privacy Protection Service That Creates Premium Billing and Increased Revenues*

Responding directly to your customers' specific needs, the AT&T Privacy/Data Product is a high performance AUTOPLEX System feature designed to enhance customer service, attract new customers and generate increased per subscriber revenue by collecting premium charges for a premium service — voice and data privacy

**AT&T CTS 1620 PRIVACY/DATA ACCESSORY SPECIFICATIONS**

| | |
|---|---|
| Voice and Data Encryption | Proprietary Digital Encryption Protocol |
| **Data Features:** | |
| **Transmission Rate** | 300, 1200, or 2400 bits/sec |
| **Communications Code** | 5-8 data bits; 1-2 stop bits; even, odd, or no parity |
| **Communications Mode** | Half or full duplex selectable |
| **Flow Control** | XON/XOFF optional |
| **Error Control** | ARQ with CRC-16 checking gives BER lower than 1 in a million over radio link |
| **Compatibility** | Standard dial-in ports equipped with AT&T 2212 or 2224 modems (includes Bell 103 and 212A standards) or equivalent |
| **Auto Dialing** | Ability to store and dial up to 8 telephone numbers |
| **Supply Voltage** | 13.6 Vdc (negative ground) |
| **Battery Drain** | 150 mA standby<br>2.0 A active |
| **Size** | 12 1/2" x 6 3/4" x 4 3/4" with base |
| **Weight** | 8 lb. 8 oz. |
| **Cables:** | |
| **To Control Head** | Existing 24-wire AMPS data cable |
| **To Transceiver** | New 36-wire AMPS data jumper provided |
| **Power from Battery** | Existing 4-wire AMPS power cable |
| **Power to Transceiver** | New 4-wire AMPS power jumper provided |
| **RS-232C** | Optional cable provided by customer to match data terminal if used. Unit has DB-25S connector. |

For additional information or to order the AT&T AUTOPLEX Privacy/Data Product, please contact your AT&T Sales Representative.

©1985, AT&T Technologies, Inc.
All Rights Reserved
Printed in the U.S.A.

AT&T Network Systems
Marketing Communications
2151D

AT&T
The right choice.

# TESTIMONY OF
# RICHARD L. BROWN, GENERAL COUNSEL
# SATELLITE TELEVISION
# INDUSTRY ASSOCIATION, INC./SPACE
# BEFORE THE
# SUBCOMMITTEE ON COURTS CIVIL LIBERTIES, AND THE ADMINISTRATION OF JUSTICE OF THE COMMITTEE ON THE JUDICIARY, HOUSE OF REPRESENTATIVES

**January 30, 1986**

Mr. Chairman, members of the Subcommittee, I am General Counsel for SPACE, The Satellite Television Industry Association, Inc. SPACE is pleased to submit these views for the record on H.R. 3378, the "Electronic Communications Privacy Act of 1985." SPACE is the trade association representing manufacturers, distributors, sellers and owners of home satellite earth station equipment. Today, over a million and a half homes throughout the United States enjoy their own satellite earth station equipment. Through the use of this exciting technology, Americans in even the remotest corners of our land have been able to fully participate in and benefit from a revolution in communications. We understand that H.R. 3378 was not intended to interfere with the ability of home owners with satellite earth stations to view satellite programming and was not meant to change the status of the existing law. We have a suggestion on how that goal can be more clearly reached.

Through the use of home satellite antennas, individuals are able to view scores of channels of programming, much of which was undreamed of just a decade ago. This programming consists of information and entertainment channels, television network programming, sports programming, news and financial programming, the proceedings of the Congress, over a half-dozen specialty religious services, travel and information services, as well as foreign language broadcasts.

Last year, after closely examining the growth of this home satellite industry and the many benefits it provides, particularly to unserved rural areas, Congress specifically modified provisions in the Communications Act to clarify that home viewing of various satellite television programming violated no law. These amendments were contained in Public Law 94-549, The Cable Telecommunications Policy Act of 1984. That law clarified the legality of ownership, sale and use of home satellite antennas. Under that law, the providers of satellite programming who wish to be compensated for viewing of such programming may scramble their programming or negotiate a marketing system for viewing unscrambled programming.

The use of home satellite earth stations to view television programming is a rapidly growing and evolving practice. What types of programming may be viewed by home satellite earth station owners will be no doubt the subject of future legislative and judicial proceedings. To date, two subscription services have scrambled their signals. Many questions and problems remain concerning the costs of the service and the descrambling equipment, who will be authorized to market those signals, whether decoders in sufficient quantities will be available for consumers who desire them and the compatability of scrambling units with existing satellite equipment.

This uncertainty has caused the introduction of new legislation this year. H.R. 1769, authored by Congressman Judd Gregg and co-sponsored by some 60 other Congressmen would impose a two-year moratorium on scrambling of satellite programming. H.R. 1840, authored by Congressman W. J. (Billy) Tauzin provides for access to scrambled signals by home satellite earth station owners at reasonable prices. It, too, has 60 co-sponsors. H.R. 3989 was recently introduced to address efforts by the cable industry to control price and availability of satellite television services. Hearings on these issues are scheduled for March 6, 1986, before the Telecommunications Subcommittee, chaired by Congressman Timothy Wirth.

In light of Congress' action last year and the pendency of the other legislation discussed above concerning home satellite earth stations, we agree that H.R. 3378 should be neutral on the subject and should reflect accurately the existing state of the law. We submit that the proposed exemption does not meet fully meet this objective.

Section 705(b) specifically modifies former Section 605 by clarifying that home viewing of satellite cable programming is legal. As is more fully discussed in the letter which is attached hereto, and made part of this testimony, home satellite viewing of other types of television programming, such as network feeds or non-network broadcasts, were not made illegal by virtue of their not being specifically mentioned in Section 705(b). Home viewing of such programming depends on judicial interpretation of the provisions of Section 705(a), former Section 605. See attached letter.

We respectfully request that the legislation be amended to specify that conduct with a home satellite antenna which does not violate Section 705(a) (as well as 705(b)) is not intended to be prohibited by H.R. 3378. Absent such an amendment, a future court could easily misconstrue the provisions of H.R. 3378 and make a finding, inclusio unius est exclusio alterius, that use of a home satellite antenna to view other than "satellite cable programming" was prohibited by H.R. 3378.

To clarify this matter, we urge that Section 101(g)(iii)(II) be rewritten as follows:

> (g) It shall not be unlawful under this Chapter for any person —
>
> . . .
>
> . . .
>
> (iii) to engage in any conduct which —
>
> (I) which is prohibited by section 633 of the Communication Act of 1934; or
>
> (II) with respect to satellite earth stations which is lawful under the provisions of section 705(a) or section 705(b) of the Communication Act of 1934.

By this amendment, it will be clear that if viewing of particular satellite programming is lawful under the provisions of Section 705(a) or Section 705(b) of the

Communications Act of 1934, it is not made unlawful by implication of the provisions of H.R. 3378. This is not intended in any respect to change the substance of Sections 705(a) or (b) of the Communications Act. This proposal is merely to have the provisions of H.R. 3378 reflect the fact that the law governing receipt and divulgence and use of home satellite communications is indeed governed by both Sections 705(a) and (b) of the Communications Act. Adoption of our proposal would make H.R. 3378 fully consistent with these facts and the state of the law.

Respectfully submitted,

**THE SATELLITE TELEVISION INDUSTRY ASSOCIATION, INC./SPACE**

By: ____________________________
Richard L. Brown, General Counsel

Counsel: Richard L. Brown, Esq.
Brown & Finn, Chartered
1920 N Street, N.W.
Suite 510
Washington, D.C. 20036
(202) 887-0600

LAW OFFICES
BROWN & FINN
CHARTERED
SUITE 510
1920 N STREET, N.W.
WASHINGTON, D.C. 20036

(202) 887-0600

January 28, 1986

The Honorable Robert W. Kastenmeier, Chairman
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Kastenmeier:

We have reviewed a copy of a letter to you from Jack D. Smith, General Counsel of the Federal Communications Commission, concerning the applicability of Section 705(a) to network television feeds. We believe that Mr. Smith's letter does not fully address matters of great concern to the Congress and to millions of Americans.

Initially, Mr. Smith concludes that if Section 705(a) applies to network satellite feeds, unauthorized "interception" of those signals by homeowners could lead to civil or criminal actions under the statute. A close analysis of the language of Section 705(a) will demonstrate that the statute does not, under any circumstance, proscribe or penalize the mere "interception" of any signal. Section 705(a) is divided into four independent clauses. As the Supreme Court has noted, each of these clauses must be given independent effect, and it cannot be presumed that the subtle difference in the wording in each clause was inadvertent. Weiss v. United States, 308 U.S. 321 (1939). The first clause prohibits persons employed in communications enterprises from divulging or publishing the contents of communications except through authorized channels to authorized receivers. The second clause prohibits persons "not being authorized by the sender" from "intercepting" any radio communication and "divulg[ing] or publish[ing]" its contents to any person. The third clause prohibits persons "not being entitled thereto" from "receiv[ing] or assist[ing] in receiving "any communication and "us[ing] such communication (or any information therein contained) for his own benefit or the benefit of another not entitled thereto." The fourth clause prohibits persons receiving intercepted radio communications from "divulging" "publishing" or "using" their contents. The Supreme Court has held that the first and third clauses of the statute apply only to the receipt and unauthorized use of radio communications by employees of communications agencies. Weiss v. United States, supra; see also Sablowsky v. United States, 101 F.2d 183 (3d Cir. 1938). Thus, homeowners who "intercept" communications can be held liable, if at all, under the second clause of the statute, which prohibits only "interceptions" coupled with "divulgences" to third parties.

Secondly, while Mr. Smith correctly points out that the applicability of the proviso to Section 705(a) (which excludes from the statute's coverage signals transmitted "for the use of the general public") depends primarily upon the "intent" of the sender, Mr. Smith presumes that intent on behalf of the networks rather than searching for any objective manifestation of its implementation, as almost every court called upon to decide this issue has done. In *Chartwell Communications Group, Inc. v. Westbrook*, 637 F.2d 459 (6th Cir. 1980), the lead case cited for the proposition that protection of a signal under Section 705(a) depends in large part upon the intent of its sender, the court stressed the necessity of finding clear, objective evidence of a sender's intent as manifested by its attempt to protect its signal from interception:

> Mass appeal and mass availability are factors which weigh in favor of finding that a particular activity is broadcasting. However, those factors may be negated by clear, objective evidence that the programming is not intended for the use of the general public. . . . The fact that STV is transmitted in such a manner that the signal is meaningless without the use of special equipment negates a finding that STV is intended for the use of the general public.

637 F.2d at 465. Courts have recognized that they "might face difficulties" in enforcing the statute to proscribe the use of equipment that has the capacity to receive authorized as well as unauthorized signals. *HBO v. Advanced Consumer Technology*, 549 F. Supp. 14, 25 (S.D.N.Y. 1981). The Commission itself has stated:

> It has long been the Commission's view that the initial responsibility for signal protection should be on the signal originator who is in the best position to protect the signal against unauthorized interception and use.

*Michael Reynolds*, 89 F.C.C.2d 450, 455 (1982).

Because network television feeds are, for the most part, unencrypted, homeowners may easily receive and view those signals with equipment they are clearly authorized to use to view satellite cable programming under Section 705(b). Mr. Smith's view is not supported by the one case which has been decided since passage of the Act and which addressed issues concerning the liability of retailers of home earth station equipment under Section 705. In that case, the court dismissed a suit against the retailer of home satellite equipment which was used to receive both satellite cable and network feeds. The court found:

> Even before Congress acted to amend the act to permit the manufacture, distribution, sale and use of earth stations under certain circumstances, this court held the firm belief that former Section 605 could not be used to strangle enterprises involving today's modern technology which enables home viewing of satellite-transmitted programming through the use of earth station satellite dishes.

AirCapital Cablevision, Inc., et al. v. Starlink Communications Group, Inc., et al., No. 83-1997-K (D. Kan., May 23, 1985), slip. op. at 3.

Finally, it should be emphasized that the satellite viewing rights provisions embodied in Section 705(b) were not intended to remove any other defenses to actions brought against viewers of television programming by satellite. Addressing this issue, Senator Goldwater, author of the Senate Bill, stated:

> . . . I will emphasize that nothing in Section 705 is meant to foreclose consideration by the courts of whether particular transmissions not clearly satellite cable programming are considered for use of the general public or are protected by the First Amendment and thus, exempt from the provisions of Section 705. This means that activities presently legal under Section 605 are not made illegal simply because they are not defined in the new Section 705(b).

130 Cong. Rec. S. 14284 (October 11, 1984).

These views were reiterated in the House by then Congressman, now Senator, Albert Gore, who stated:

> It is important to clarify the law on this important area of satellite communications to the home and by doing so we are not meaning to pass judgment on any case that was or was not decided in the past under section 605 of the Communications Act of 1934. Nor are we passing judgment on any activities or programs not specified in the legislation. It is also my understanding that the provisions of H.R. 4103 concerning home satellite Earth station viewing of cable programming are not meant to change any copyright law under title 17 of the United States Code or any rule, regulation or order thereunder, or any other such law.

130 Cong. Rec. H. 10443 (October 1, 1984) (Remarks of Rep. Gore).

To date, no court anywhere has found that home viewing of television network feeds is prohibited by the provisions of Section 705(a) or its predecessor Section 605. Mr. Smith's view that such viewing could lead to liability even if the signal is not scrambled and even if the communications are not divulged, is not supported by the statutory language or legislative history of Sections 705(a) and (b) and certainly not even by one single case under Section 705(a) or former Section 605.

Sincerely,

Richard L. Brown
**Brown & Finn, Chartered**
Counsel to the Satellite Television
Industry Association/SPACE

cc: Jack Smith, Esquire
General Counsel
Federal Communications Commission
1919 M Street, N.W., Room 614
Washington, D. C. 20554

RLB:cmm

JAN 17 1986

Brigham Young University
J. Reuben Clark Law School

January 10, 1986

Hon. Robert Kastenmeier
U.S. House of Representatives
Committee on the Judiciary
Washington, D.C. 20515

Dear Congressman Kastenmeier:

This letter is in response to your request of September 16, 1985 asking for my comments on H.R. 3378. My apologies for the delay in filing this report with you.

Overall, I believe that H.R. 3378 effects several significant improvements in the area of non-consensual Title III electronic surveillance. Among the amendments I endorse are those providing for mandatory progress reports, adequate specification of investigative alternatives, cross-jurisdictional mobile interception, and required court authorization for installation of electronic devices. In addition, it is apparent that H.R. 3378 successfully closes existing legal gaps insofar as other types of electronic searches (e.g. computer data banks) are concerned. These are, indeed, significant legislative improvements.

Nevertheless, to the extent that other issues raised by my hearing testimony remain untreated (e.g., disclosure of eavesdropping matters to grand jury witnesses, surveillance of unknown parties, minimization, retroactive and prospective amendments, and a good faith exception), I am somewhat disappointed. Given the complexity of the issues involved, however, I will make no effort to discuss those points anew. In addition, I am deeply troubled by those aspects of H.R. 3378 which impose a new set of standards on investigations involving pen registers and tracking devices. My opposition to these standards is set forth below as part of an overall commentary on the bill. For organizational purposes, my remarks are presented seriatim according to the bill's pagination.

Brigham Young University Provo, Utah 84602 (801) 378-4274

## Specific Comments

p. 3, line 12: This provision appears to be in error. It seems to provide that it is not unlawful to engage in conduct prohibited by the Communication Act of 1934. If the word "not" is intended, the legislative commentary should clarify what purposes are to be served by this provision.

p. 6, line 1: This provision is ambiguous. Does it penalize those who access electronic communications systems or does a violation require both access and obtaining or altering a electronic communication?

p. 6, line 20: Why are all other violations merely subject to a $5000 fine and/or six months imprisonment? Suppose that a police officer intentionally violates these provisions. Shouldn't his penalty be at least as great as that presently authorized in section 2511 of Title III?

p. 6, line 22: It is not clear whether criminal penalties are available for violations of this section. None are specified.

p. 7, line 16: What purpose is served by requiring successful applicants for interceptions to file additional requests for disclosure. At best, this is an unwieldy process. Moreover, how are law enforcement officers to handle information acquired through such interceptions? Must disclosure authorization be obtained before such information can be communicated to other investigators? The present language seems to suggest such an illogical result.

p. 8, line 6: This language effects a drastic change in present law, since it removes such information from the scope of a grand jury subpoena. As such, the provision goes substantially beyond Supreme Court interpretations of the Fourth Amendment. *Cf*. *Smith v. Maryland*, 442 U.S. 735 (1979).

p. 9, line 17: The bill includes a good faith defense for civil actions; given both prevailing Supreme Court jurisprudence (see *United States v. Leon*, 104 S. Ct. 3405 (1984)) and the complexity of the law, a comparable provision is in order for criminal cases involving the statutory suppression sanction.

p. 9, line 19: Once a violation is found to be within the statute of limitation, do previous violations constituting part of the same pattern of illegality likewise come within its scope?

p. 10, line 21: Given the President's Commission on Organized Crime's recent report on the money laundering problem, Bank Secrecy Act violations should be included in the list of predicate crimes.

p. 11, line 9: This provision should be clarified to indicate that law enforcement officers are not required to utilize each of these techniques as a prerequisite to surveillance.

p. 12, line 7: What does "no other less intrusive means reasonably available" mean in this context? Suppose other means exist but are either much more expensive or would not result in interceptions of optimal quality? Also, the provision fails to address the need to re-enter the premises to make repairs and to remove the listening device upon termination of surveillance.

p. 12, line 17: This provision is a real improvement but raises several questions. First, why is no reference made to the judge's need to review compliance with minimization requirements? This is a crucial omission. Second, what if evidence of a new crime has been intercepted? How does this provision relate to existing section 2517 standards and procedures? For example, does it mean that there is no need to comply with them until the progress report is filed?

p. 13, line 4: This provision ought to be eliminated in its entirety. Thus far, no one has advanced a rational argument in support of a sealing rule. As I indicated during my testimony, this requirement in no way adds to the security of any taperecordings; unfortunately, sealing violations have been responsible for the suppression of evidence in far too many cases.

p. 13, line 10: The effective date provision may cause confusion by changing the rules in midstream for warrants already in existence. Perhaps the provision should be made applicable only to new orders.

p. 16, line 8: This provision unduly restricts the availability of pen registers. Pen registers, as well as their analogues -- toll records, are oftentimes the first investigative step to be taken in conducting an organized crime inquiry. At that time, the investigators are searching for patterns of criminal activity which cannot otherwise be analyzed. Reasonable cause as to a specific crime may not be developed until this process has been completed. For this reason, the provision is unsound. It also imposes a standard which exceeds present Supreme Court requirements. Smith v. Maryland, supra.

p. 16, line 10: The probable cause standard in this context is too demanding and is being applied much more broadly than the Supreme Court has required. See United States v. Karo, 104 S. Ct. 3296 (1984). The provision ignores the fact that tracking devices are often an important means of obtaining probable cause for subsequent searches and seizures. Also, suppose that the police need to track a suspected kidnapper as to whom probable cause is lacking? This provision would preclude them from using the best available techniques to accomplish their goal.

p. 17, line 21: The time period is geared to the investigative objective, but this portion of the bill does not explicitly require the objective to be specified.

p. 22, line 3: This provison imposes a heavy burden on law enforcement, as it apparently requires that any person monitored via a pen register be given inventory notice. Read literally, this provison may have the effect of requiring notice to be given to thousands of persons -- since a telephone being monitored in this way may record the making of dozens or even hundreds of calls in a single day. Also, what is to be the remedy for violation of this provison. None is specified.

p. 23, line 4: This provision should be eliminated in its entirety. It serves no purposes and will pose an intolerable burden on law enforcement. Title III admittedly has a comparable provision, but it was imposed because of a clearly perceived need to monitor the extent to which a very intrusive investigative technique was being used under court authorization. As a former organized crime prosecutor, I can attest that the compilation of the Title III reports is extremely time-consuming. Nevertheless, since most prosecuting agencies do relatively few such surveillances annually, the task is still manageable. In contrast, for example, the use of pen registers is relatively commonplace; as such, the filing of annual reports would be a mind-boggling ordeal. Moreover, it would serve no purpose, as there is no indication (comparable to the Title III situation) that the system is presently being abused in this manner.

p. 26, line 5: Only civil sanctions are specified for violations of this provision. This implies the absence of a suppression sanction. That, of course, would be an appropriate result since it is by no means clear what could even be suppressed in such situations.

p. 27, line 14: This provision would have the effect of requiring all of the states to pass legislation regulating pen registers and tracking devices. Since there is no indication that the state systems are in need of reform, this provision is both unwise and an arrogation of federal authority.

p. 27, line 21: What about state investigations? Since the bill contemplates state application, corresponding state language should be added.

p. 28, line 5: The definition of tracking device may undercut all you hope to achieve in this context, as it is geared to the expectation of privacy standard. Under prevailing Supreme Court jurisprudence, persons may often be tracked without warrant when there is no such expectation. See United States v. Karo, supra; United States v. Knotts, 460 U.S. 276 (1983). As such, you are now tying yourself into Supreme Court case law rather than going beyond that standard.

Thank you for inviting me to provide the above commentary. At times, my remarks may appear unduly blunt, but that is simply because space and time limitations necessitate that I get right to the point. If any of your staff personnel would like to contact me with follow-up questions, please feel free to have them do so.

Sincerely,

Michael Goldsmith

Michael Goldsmith
Associate Professor
of Law

AMERITECH
AMERICAN INFORMATION TECHNOLOGIES

BRUCE J. EGGERS
Director — Congressional Relations

Suite 730 — Washington Square Bldg.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
202/955-3070

December 17, 1985

The Honorable Robert W. Kastenmeier
Chairman, Subcommittee on Courts,
Civil Liberties, and the
Administration of Justice
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Kastenmeier:

Thank you for your thoughtful letter of November 15th, enclosing a copy of the November 11th draft of the "Electronic Communications Privacy Act of 1985," H.R. 3378. Bob Kitzinger, Director-Corporate Security for Ameritech, has had an opportunity to review this latest version and his comments are enclosed. As you know, Ameritech is the holding company for Wisconsin Bell and other Bell operating companies around the Great Lakes.

As his letter indicates, Mr. Kitzinger is pleased with the fine efforts that have been made to improve the legislation. For your consideration, he has four, evidently minor, suggestions that would further strengthen the bill.

I join Bob Kitzinger in thanking you, David Beier, and Deborah Leavy for your accessibility and extraodinary initiative in seeking input from the telephone industry on this important legislation. You have our best wishes as H.R. 3378 and S. 1667 advance through the legislative process.

Sincerely,

Bruce J. Eggers

Enclosure

cc: ✓David Beier
Deborah Leavy

DEC 12 1985

AMERITECH

**R. W. KITZINGER**
Director-Corporate Security

30 South Wacker Drive
Chicago, Illinois 60606
312/750-5155

December 6, 1985

Mr. B. J. Eggers
Director - Congressional Relations
Ameritech - Suite 730
1050 Connecticut Avenue, NW
Washington, DC 20036

Re: H.R. 3378 (Modified)

Dear Bruce:

I have looked at the November 11 re-write of the "Electronic Surveillance Act of 1985" provided to you by Rep. Kastenmeier. I believe that the Committee on the Judiciary has honestly tried to incorporate our suggestions into their current version and that, indeed, they have cured my most pressing concerns.

This bill now tracks quite well with our recommendations as articulated by Jim Golden in his letter of October 31 to David Beier. I believe Ameritech could accept the bill if it were passed in its present version. Given an opportunity, I would suggest a little further attention to the following:

- Section 3123 (b)(1)(3) includes a typo. "Identify" should read "Identity."

- Section 3123 (d) now specifically states that (we are) "not required to make such disclosure at any time." However, this whole reference is clumsy and confusing. Since Section 3126 provides for notification by the Court under a structured procedure, it is unnecessary to have this 60 day reference in the statute at all. I suggest that the paragraph be reduced to end at line 16 where "shall not disclose the existence of the pen register" can effectively close the section.

- Section 3125 (b) refers in line 5 to "electronic communications system." "System" should be replaced by the term "provider" in this sentence.

- Section 3125 (c) states that the provider should be compensated "for reasonable expense incurred." This reference is limited and subject to interpretation of "expenses." I suggest the phrase be stricken and the sentence amended to read: ... shall be reasonably compensated for such assistance in providing such facilities or service.

Thank you for continuing to keep me current on the changes in this proposed legislation. I think we should express our appreciation to the sponsors for their continued willingness to cooperate with us in making changes necessary for our industry.

Sincerely,

Bob

LAW OFFICES
BROWN & FINN
CHARTERED
SUITE 510
1920 N STREET, N.W.
WASHINGTON, D.C. 20036

(202) 887-0600

December 3, 1985

The Honorable Robert W. Kastenmeier, Chairman
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice
Committee on the Judiciary United States
House of Representatives
Washington, D.C. 20515

Dear Chairman Kastenmeier:

SPACE, the Satellite Television Industry Association, is the trade association representing the owners, sellers, and manufacturers of home satellite earth station reception equipment. We deeply appreciate the sensitivity of the Subcommittee to home satellite earth station issues.

As you know, last year Congress passed the Cable Communications Policy Act (Pub. L. No. 93-549) in which it clarified the legality of home earth ownership and use. This year two bills, H.R. 1769 and H.R. 1840, have been introduced which also address various issues concerning reception of satellite television programming. It is our understanding that H.R. 3378 is not intended to address these issues. We are pleased to submit some suggestions of how to further reach this objective.

Proposed Section 101(g)(iii)(II) provides an exception from liability for those who are engaged in any conduct which is exempted from the application of Section 705(a) of the Communications Act of 1934, by Section 705(b) of that Act. While this provision does clarify that H.R. 3378 is not intended to change the law which passed last year, we respectfully suggest an additional modification. Home viewing of satellite television services may be specifically exempted from liability by the provisions of Section 705(b) because they are not classified as "satellite cable programming" under the definition contained in Section 705(c)(1). Nevertheless, such services may otherwise be exempt from the provisions of Section 705(a). For example, the provisions of Section 705(a) may not apply because the services are transmitted for "use of the general public." Also, for Section 705(a) to be violated there must be an "intercept[ion] and divulge[nce]" or reception and "use" which may not exist.

December 3, 1985
The Honorable Robert W. Kastenmeier
Page Two

To clarify this matter, we urge that Section 101(g)(iii)(II) be rewritten as follows:

(g) It shall not be unlawful under this Chapter for any person —

. . .

. . .

(iii) to engage in any conduct ~~which~~ —

(I) which is prohibited by section 633 of the Communication Act of 1934; or

(II) with respect to satellite earth stations which is lawful under the provisions of Section 705(a) or Section 705(b) of the Communication Act of 1934.

Thank your for your consideration of our concerns in these matters.

Sincerely,

Richard L. Brown
**Brown & Finn, Chartered**
Counsel to the Satellite Television
Industry Association/SPACE

RLB:cmm

The Source INFORMATION NETWORK

Leslie C. Seeman
General Counsel

November 21, 1985

The Honorable Robert W. Kastenmeier
Committee on the Judiciary
Subcommittee on Courts, Civil Liberties
and the Administration of Justice
2137 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Kastenmeier:

Source Telecomputing Corporation ("STC") greatly appreciates your invitation to submit comments on the proposed Electronic Communications Privacy Act of 1985, H.R. 3378 and S. 1667. STC strongly supports the intent of legislation designed to update the nation's laws to protect telecommunications privacy. STC operates The Source, an online information and communications service whereby personal computer users can access a variety of different databases and communications services like electronic mail. As you may know, significant public attention has recently been focused on STC's efforts to protect from improper disclosure to government authorities, the information contained in private electronic mail files of our subscribers. We are therefore particularly appreciative of efforts to extend statutory protection to the privacy of those types of communications.

We believe, however, that there are at least two areas in which the provisions of H.R. 3378 and S. 1667 should be revised. First, we have identified several loopholes in the bill as drafted that would make unlawful what are today the ordinary and necessary activities of service providers in the normal course of business. Second, we believe the bill must recognize the national nature of services such as ours, and preempt individual state legislation dealing with service provider maintenance and disclosure of customer information. Each of these points is discussed below.

1616 Anderson Road, McLean, Virginia 22102 703/734-7500
The Source is a service mark of Source Telecomputing Corporation, a subsidiary of The Reader's Digest Association, Inc.
The Source Services are offered in participation with Control Data Corporation.

I. Proposed Text Revisions (All changes are cited to the September 12, 1985, H.R. Discussion Draft.)

A. On page 6, lines 2-3:

Substitute for the words "a user" the words "an authorized user." This change is necessary to prevent unauthorized users, who are nonetheless "users," from "authorizing" and thus legalizing improper access by one another. It will probably also be necessary to include a definition of the term "authorized user," which makes clear that such a user is a bona fide customer of the service provider in good standing, and is providing authorization with respect to information or files assigned to such user.

B. On page 6, line 23:

Add after the word "communication" the words "from an authorized user." This change is necessary in order to ensure that legal privacy protection only applies to communications from authorized users. Hackers should not be subject to this type of protection; indeed, the contents of their communications often must be divulged--and removed from the system--in connection with routine service provider security investigations and enforcement activities.

C. On page 6, line 25:

Add after the word "addressee" the words "or intended recipient." This change is necessary because certain communications (e.g. communications to database providers on automated order forms) do not necessarily have an addressee.

D. On page 7, line 5:

Add after the words "user originating such communication" the words "or the recipient." This change is necessary to permit recipients to authorize disclosure of the contents of communications sent to them. This type of disclosure may legitimately be required in connection with technical assistance activities, record retrieval, resolution of billing disputes, and security investigations.

E. On page 7, line 6:

Delete the word "employed" and insert the words "whose services or facilities are used." This change is necessary because communications are frequently channeled through a series of independent service providers, who are not "employed" by one another.

F. On page 7, lines 10-11:

Delete the words "to a user of the electronic communication service." This change is absolutely essential in order to permit service providers legitimately to disclose communications in connection with routine business activities not related to the provision of a service to a particular user. For example, disclosure may be necessary in connection with security investigations and enforcement activities, which are necessary administrative functions performed by the service provider on its own behalf and on behalf of the user population as a whole, rather than services provided to any specific user.

G. On page 8, line 9:

Delete the entire line and insert in lieu thereof the following: "to one or more communications made to or through that service or relating to authorized users of that service." This change is necessary to close a loophole in the provision as drafted, which would protect from disclosure to the government only records relating to a "particular" communication. There are numerous subscriber records that should be subject to privacy protection, but do not relate to a "particular" communication, such as summary records of database usage, time of usage, and billing status. Without this proposed revision, a government subpoena could request all service provider records relating to a given subscriber (and it is not unlikely that government subpoenas would be drafted in this form), and it could be argued that such records are not subject to privacy protection since they do not relate to a "particular communication."

H. On page 8, line 22:

Delete the words "or used." This phrase is too broad and vague and does not relate to any substantive prohibitions.

## II. Preemption

In our view, it is essential that any federal communications privacy bill contain a preemption provision that would preclude service providers from being subjected to conflicting state standards. Telecommunications networks such as that operated by STC are inherently interstate--indeed worldwide--services. Any user can access The Source from equipment located in any state and user communications are channeled over wires crossing through a number of states. Yet the services on The Source are the same, regardless of the user's location or channels of access.

It would be manifestly unfair and impracticable from a business standpoint to require service providers to segment their operations to comply with the different requirements of different state laws. Without a preemption provision, the practical effect would be that service providers would have to conform their operations to comply with the most stringent state law, which would then have the de facto effect of national law, superseding the carefully crafted balance of rights and duties in this bill. Even monitoring 50 state laws would be costly; providing legislative input to individual states would be beyond our capabilities.

Sincerely,

Leslie C. Seeman
General Counsel

LCS/kkh

c: Senator Patrick Leahy

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS
WASHINGTON, D.C. 20544

L. RALPH MECHAM
DIRECTOR

WILLIAM JAMES WELLER
LEGISLATIVE AFFAIRS
OFFICER

October 31, 1985

Mr. James C. Murr
Office of Assistant Director
for Legislative Reference
Office of Management and Budget
Washington, D.C. 20503

Dear Mr. Murr:

This is in response to your letter of October 22, 1985, requesting our views on H.R. 3378, the Electronic Communications Privacy Act of 1985. We appreciate the opportunity to comment.

Neither the Judicial Conference nor any of its Committees has yet had an opportunity to review the specific provisions of this bill. Pending review by the conference, we do express concern as follows about the workload impact that would result if the proposal is enacted:

1. Clearly, in extending to various modern technological equivalents of telephone calls and telegrams the same protections afforded by current law as to such communications, Congress will be increasing the workload of the Federal judges who are required to review applications for warrants and issue orders granting requests to intercept communications. It is possible that the number of such additional applications will be substantial on a national basis, and that a disproportionate share of these applications may fall on judges in major metropolitan areas.

2. Provisions of this bill would seem to limit the use of United States magistrates as authorized issuing officers. To the contrary, provisions should be made to authorize magistrates to issue any orders involving electronic communication in the same way they are authorized to issue search warrants. Any additional restrictions on the role of magistrates in this area will, of course, simply increase the judge's workloads further.

3. The provisions in the bill which require that reports be made to the Administrative Office by the courts on applications and orders for pen registers and tracking devices would also result in additional work for the courts (in particular,

the clerks' office), and the corresponding report by the Director to Congress will similarly create more work for this agency. A total of 801 wiretap authorizations were reported to us for calendar year 1984. We would estimate that if this bill is enacted the number of reports would triple at the minimum. In addition, this bill will require prosecuting attorneys to spend more time preparing reports for the Administrative Office.

Thank you for the opportunity to comment upon this legislation.

Sincerely,

Christy E. Massie

Christy E. Massie
Counsel

October 31, 1985

# MEMORANDUM

Re: Senate Bill No. 1667; House Bill No. 3378;
The "Electronic Communications Privacy Act
of 1985"

Following are suggested changes to the text of H.R. 3378, the "Electronic Communications Privacy Act of 1985":

1. The need for conforming amendments to the Communications Act of 1934 (47 U.S.C. § 201, et seq.).

a. The Bill's proposed definition of "Electronic Communication" (as a substitute for the term "wire communication") changes, at least facially, those communications which are protected from unauthorized interception under Title 18.

However, the Bill fails to conform the provisions of Section 705 of the Communications Act of 1934 (47 U.S.C. § 705) to the new terminology. Section 705 generally prohibits the divulging or publishing of the existence, contents, substance, purport or effect of communication by wire or radio "[e]xcept as authorized by Chapter 119, Title 18 . . ." Current law thus provides a savings clause for what would otherwise be a violation of § 705. The new Bill would alter the provisions referred to in the savings clause so that the scope of protection provided by the savings clause does not conform to the criminal prohibitions in § 705. This problem is easily cured by a conforming amendment to § 705. In the absence of such an amendment, Telephone Companies could face criminal liability under § 705 for acts performed in accordance with Chapter 119.

b. A similar conforming amendment is required in § 705 of the Communications Act because of the Bill's proposed change in the definition of the term "content" (18 U.S.C. § 2510(8)). That proposed change would delete the word "existence" from those contents which are protected against unauthorized disclosure. The interception of "any [other] information concerning the identity of the parties to an electronic communication" or "the substance, purport, or meaning" of that communication would still remain a crime unless authorized pursuant to Chapter 119. Again, however, there is a need for conforming amendment for § 705 of the Communications Act. Under that statute, the disclosure of the existence of a communication is a crime unless authorized pursuant to Chapter 119. The current Bill would, if passed, eliminate the need for any authorization regarding disclosure of the existence of a communication and would thus expose Telephone Companies to the application of inconsistent statutes.

The relevant text of a conformed § 705 should then read as follows:

> **§ 705. Unauthorized publication or use of communications**
>
> **(a) Practices prohibited**
>
> Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign electronic communication . . . shall divulge or publish the contents, substance, purport, effect, or meaning thereof, except . . . . No person not being authorized by the sender shall intercept any electronic communication and divulge or publish the contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign electronic communication and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted electronic communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of any other not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any electronic communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator."

2. The Bill should include a definition of the term "Electronic Communications System." That term appears in several places throughout the Bill (e.g., proposed § 2511(2)(g)(i) and proposed § 2511(3). The necessity for

such a definition is particularly apparent with regard to § 2511(3) because that section would impose criminal liability for accessing an electronic communication system with the subsequent obtaining or altering of a communication stored therein. In light of changing technology, the lack of a definition for this critical term could result in the holding that the provision was itself unconstitutionally void for vagueness.

3. Proposed § 2511(2)(g)(i) should be amended to narrow the scope of the exception otherwise established by this section. The proposed new § 2511(2)(g)(i) disclaims any criminal liability for the interception of an electronic communication made through a system "designed so that such electronic communication is readily accessible to the public." The obvious purpose of this provision is to clarify that no crime is committed when a person intercepts a communication which is intended to be intercepted, e.g., "Dial-a-Prayer" recordings. However, the wording of the exemption is troublesome. An electronic communications system could be designed, albeit poorly, so that communications over that system can, in fact, be intercepted (even unintentionally) by the public. Certain designs of cordless telephones are an example. Such telephones were not designed with the intention that they be intercepted by the public, but in fact their design is that such interception is possible through the use of an electronic device (e.g., cordless telephone conversations can be heard over Citizen's Band or Amateur radios or certain UHF television stations). Whether these types of "interceptions" fall within the scope of the exception as being "readily accessible to the public" is unclear. A better course would be a narrowing of the exception to one which permits interception only if the electronic communications is over a system which was designed for the purpose of public access.

4. Proposed § 2511(2)(h)(ii) should be amended to clarify the intended exception for Telephone Companies which would permit the use of pen registers in investigations of toll fraud or abuse of service situations (e.g., annoying and anonymous calls). This exception is suggested in the current draft of subsection (h)(ii) but requires greater specificity.

The text of a revised § 2511(2)(h)(ii) should be as follows:

> "(ii) for a provider of electronic communication services to record the placement and completion of a telephone call in order to protect the rights and property of such provider or to protect such provider, or a user of that provider's service, from abuse of service."

As we have previously described, pen registers (or Dialed Number Recorders) are employed by Telephone Company personnel in (1) internal and routine network testing operations, (2) toll fraud investigations, and (3) annoying and anonymous (abuse of service) call situations. The language of the Bill (§ 2511(2)(h)(ii)) would exempt from criminal liability only the abuse of service situations. The language suggested above expands the protection to include use of pen registers and DNRs in toll fraud investigations, including the recording by a DNR of the initial portions of fraudulently placed call to establish the fact that the call was completed (and thus a crime had been committed). Usually a recording of mutual salutations (or other introductory spoken words) by both parties to the call is sufficient and the recording terminates at that time.

5. As a point of clarification, proposed § 2511(3) would prohibit the accessing of an electronic communications system and subsequent obtaining or altering of an electronic communication while it is stored in that system. Thus, this provision does not duplicate existing prohibitions against interception of a communication while in transit. Rather, the gist of the offense is the obtaining or altering of a communication while it is stored in an electronic communication system.

Because the Bell Operating Companies are currently precluded by Court Decree and FCC rules from providing voice storage services, this provision does not appear to have any immediate impact on these companies. It could, however, have an immediate impact on non-Bell exchange carriers which are not subject to the constraints of the Modification of Final Judgment (MFJ). Likewise, this provision could impact the Bell Operating Companies in the event that the restrictions in the MFJ and FCC rules are relaxed or eliminated. In any event, however, this provision does not appear so much a restraint on Telephone Companies (or other providers of electronic communications services) as it is on the so-called "computer hackers" who access computers out of malice or for a lark.

Notwithstanding its apparent non-applicability to the Bell Operating Companies, this provision of the Bill does suffer from drafting infirmities itemized below:

- The criminal prohibitions do not apply in the case of one who is authorized to act by the entity providing electronic communications service or by a user of that service. A literal reading of this provision would appear to permit a computer hacker who is authorized by User A to obtain access to the electronic communications system subsequently to obtain or alter the communication of

BEST COPY AVAILABLE

User B. Clearly such a result is unreasonable and not intended, but nonetheless follows from a literal application of the Bill's language.

- The Bill provides more severe penalties in the event that the offense is committed for "commercial advantage, malicious destruction or damage or private commercial gain." None of these terms is defined, but they would appear to cover most of the reasons why such an offense is committed. If such a purpose is not established, the offense is subject to far less severe penalties. Whether this lack of definition is a serious drafting problem is best left to the Bill's sponsors and would not appear to be a significant problem for Telephone Companies.

6. Proposed 18 U.S.C. § 2511(3) and (4)

These sections would appear to prohibit the current practice of Telephone Companies of producing customer toll records in response to a lawful subpoena. Production of such records would be permitted only upon the conditions specified in the section, primarily pursuant to proposed § 2516 procedures.

Section 2516, in turn, is amended to permit such production only upon court order following procedures similar to those applicable to interceptions. This provision, if enacted, would materially change current practice and would appear to impose significantly higher burdens on law enforcement agencies than is currently the case. The appropriateness of such a change is a matter of public policy, the resolution of which would not materially affect Southwestern Bell Telephone Company's operations.

7. Proposed 18 U.S.C. § 2520

This section incorporates a new version of 18 U.S.C. § 2520, dealing with recovery of civil damages for violations of Chapter 119. There is one troublesome provision in the proposed § 2520:

The Bill would reduce the scope of the defense for good faith reliance on a court order. Existing law provides that: "A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law." 18 U.S.C. § 2520 (emphasis added). The Bill provides, however, only that: "A good faith reliance on a court warrant or order is a complete defense against a civil action under this section." (proposed § 2520(d))

Thus, if enacted, the Bill would reduce the scope of the defense in the following respects:

a. It would eliminate good faith reliance on a legislative authorization as a defense in such cases;

b. It would eliminate good faith reliance on a Court order or warrant as a defense in a criminal action; and

c. It would eliminate good faith reliance (whether on a court order alone or in combination with legislative authorization) as a defense in any action brought under any law other than § 2520.

The reasons for the change in the scope of the "good faith reliance" defense are not apparent. The concerns listed above are resolved simply by retaining the existing statutory language, and the Bill should be so amended.

8. Physical Entry - Section 106(d)(2)

This provision requires two minor changes:

a. The word "system" appearing in line 12 on page 12 should be deleted and the word "provider" should be inserted in lieu thereof.

b. The following language should be inserted in line 9 on page 12 between the word "officers" and the word "to":

> "into premises associated with the suspect whose communications are the subject of the court order . . ."

## Title II

### Proposed Section 3121(b)

This section generally prohibits the installation or use of a pen register or a tracking device in the absence of a court order authorizing such installation or use. Violations are punishable by prison terms (up to one year) and fines (up to $100,000), or both.

Section 3121(b) establishes an exception to the general prohibition against the use of pen registers. The exception would permit "the use of a pen register by a provider of communications services relating to the operation, maintenance, and testing of an electronic communication service." The scope of this exception is not clear. Because of the lack of clarity and in the face of the severe criminal penalties and civil liability (§ 3128) attaching to violations of the law, this provision appears to have profound--and adverse--consequences for daily Telephone Company operations.

The gist of the statutory exception is for use of a pen register when such use relates to the operation, maintenance and testing of an electronic communication service. None of these three terms is defined. However, they do not appear to permit two of the most common uses of pen registers, i.e., in toll fraud and abuse of service (harassing call) investigations.

Clearly, the permissible use of pen registers for "maintenance" and "testing" would not include the types of activities associated with toll fraud or abuse of service investigations. Thus, if the use of pen registers for these investigative purposes would be permitted under the Bill as now worded, such permission must be found in the statutory exception for pen register use "relating to the operation . . . of an electronic communication service."

As noted above, the term "operation" is not defined in the Bill. General (dictionary) definitions appear to restrict the definition to one pertaining to the mechanical functioning of a machine. Such a meaning, in this Bill, appears consistent with the other words with which the term "operation" is associated, i.e., "maintenance" and "testing." The three words have a common focus on the mechanical functioning of the electronic communication service and the detection and prevention of defects in that system.

An interpretation such as that discussed above would not permit the use of pen registers for either of the investigative purposes described above. Thus, unless the use of pen registers for such investigative purposes is permitted elsewhere, the effect of § 3121 would be to prevent Telephone Company use of pen registers in connection with toll fraud investigations or abuse of service investigations.

There is no other provision in Title II which expands the restrictive exception in Section 3121(b). The same result obtains from a reading of Title I of the Bill and the current provisions of Chapter 119. Both the Bill (Title I) and current law are limited in their applicability to Chapter 119 and thus would have no effect on the otherwise proscribed usage of a pen register under proposed Chapter 206.

Accordingly, the following amendment is proposed for § 3121(b):

> "(b) EXCEPTION - The prohibition of Subsection (a) does not apply with respect to the use of a pen register by a provider of electronic communications service, or an officer, employee or agent of such provider, in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service, the protection of the rights or property of such provider, or the protection of such provider or its customers or users from abuse of service."

## Proposed Section 3123(d)

This provision empowers the Court, at the request of the applicant, to prohibit the person owning the lines to which the pen register is to be attached from disclosing the existence of the register for at least 60 days after its removal.

Such language could be interpreted as imposing a notification obligation, albeit delayed, on the electronic communications service provider. Alternatively, the provision appears to assume that such notification would be provided immediately but for the mandated 60-day delay.

Whether notification should be required is a matter of general public policy on which telephone companies themselves possess no special expertise. The issues involve a balancing of interests, weighing possible impediments to legitimate on-going criminal investigations, on the one hand, with a desire to advise citizens of an intrusion on their privacy, on the other.

If, however, the policy decision is made to require such notification, the obligation to notify should be imposed on the entity which intruded upon the citizens' privacy and not on the Telephone Company. The latter is involved in the process only pursuant to court order and thus should not be required to assume additional duties regarding the relationship between citizen and government.

Until the Committee resolves the policy question (is notice to be required?), it is not possible to provide specific corrective language to resolve the concerns expressed above.

## Proposed Section 3124

This section establishes procedures for the emergency installation of pen registers under circumstances which do not permit obtaining an authorizing court order in advance of the installation. The procedures generally follow, with one exception, those already established in 18 U.S.C. § 2518(7) regarding the emergency installation of electronic equipment for the interception of an electronic communication.

That exception relates to the identity of the persons who are empowered to install and use the pen register in emergency situations. As now drafted, the Bill only empowers the Attorney General to authorize such conduct. This is an apparent oversight, because the parallel provisions of 18 U.S.C. § 2518(7) permit similar actions by a number of other federal and state law enforcement officials.[1]

Proposed Section 3125

This provision generally parallels those contained in 18 U.S.C. §§ 2518(4) and 2511(2)(a)(ii) regarding the court-ordered provision of assistance to the law enforcement official who has been authorized to install and use a pen register. One minor problem is evident.

The statutory duty of providing assistance to law enforcement officials is subject to an exception in Subsection (b) that persons providing such assistance shall not be required to participate in a physical entry. This is an apparent oversight since Title II does not, as Title I did for wiretaps, authorize a physical entry to install and use the pen register.

Proposed Section 3128

This section enacts a civil damage provision comparable to the provisions of the proposed amendments to 18 U.S.C. § 2520. Deviations in language from that contained in the proposed § 2520 are minor and probably curable at a technical amendment or mark-up session.

Finally, proposed § 3128(c), dealing with the defense of good faith reliance on a court order, is subject to all of the infirmities previously noted (pp. 5-6) regarding the comparable provision of Title I.

Proposed Section 3129

This section contains definitions, most of which do not appear to be of concern to the Telephone Company. Subsection (5) defines "Pen Register." That definition avoids the problems noted in earlier drafts where the pen register definition was so broad as to include Telephone Company billing equipment.

---

[1] However, *if* the Bill is enacted in its present form, a Telephone Company could face civil and criminal liability for providing assistance in emergency (non-Court order) situations when the request for such assistance originates with any official other than the Attorney General of the United States.

Although many Telephone Company security personnel employ a Dialed Number Recorder (DNR) instead of a pen register, the use of the term "pen register" does not appear to create any significant problem. The DNR is simply a more advanced device which combines the functions of the pen register with additional functions which can provide evidence of oral communication over the line to which it is attached. The fact that the DNR performs additional functions does not, however, have any legal significance. If the Bill is passed in its present form, it would apply equally to the older generation pen register and at least to the pen register function of the DNR.

James S. Golden

James S. Golden

Hubert F. Owens
General Attorney

BellSouth Corporation
675 West Peachtree Street, N.E.
Atlanta, Georgia 30375
404 529-7616

October 22, 1985

House Subcommittee on Courts, Civil
Liberties, and the Administration of Justice
2137 Rayburn House Office Building
Washington, D.C. 20515

Re: H.R. 3378 and S. 1667

Thank you for permitting us as representatives of telecommunication companies to meet with you and other staff counsel to discuss our views of this important subject. The proposed legislation does not conflict with our longstanding commitment to protect the privacy of our customers' communications. For your further consideration, I have taken the liberty of briefly restating, in writing, the major concerns that we voiced at the October 10 meeting.

The change from "wire" to "electronic" communication in the legislation could lead to an inconsistency between it and 47 U.S.C. §605, thus leaving a telephone company open to possible liability under 47 U.S.C. §605 for conduct which would be lawful under this legislation. Also, §605 would still make divulging the "existence" of a communication a crime, despite the deletion of the word "existence" in §101(a)(3) of the proposed legislation. A conforming amendment to §605 would seem to be the easiest way to clarify these situations.

Section 101(b) of the legislation contains references (at lines 12 through 16) in proposed §2511(2)(g) to parts of the Communications Act which do not exist. These appear to be typographical errors, and probably were meant to refer to §605 of the Communications Act. The concerns raised above are still valid, however, even if the error is corrected in this Section. Further, proposed §2511(2)(h)(ii) could be modified to reflect that the local telephone company may perform billing functions for an interexchange carrier which also transports the call. I would suggest that that subsection be amended to add the following underlined language: ". . . for a provider of electronic communication service to record the placement of a telephone call in order to protect such provider, any provider furnishing service toward the completion of the electronic communication, or any user of that service, from abuse of service." Also, concerning this Section, you may want to replace "a telephone call" with "an electronic communication" at line 22. As we discussed, Section 102(b) of the legislation may be inconsistent with other laws giving government agencies (e.g., the IRS) as well as state agencies the power to obtain records by subpoena. Whether this Section is intended to repeal such other laws by implication or not, it would undoubtedly cause confusion.

Section 103 of the legislation causes us great concern because it limits the exceptions from both criminal and civil liability that a telephone company presently has under 18 U.S.C. §2520 for good faith reliance on a court order or legislative authorization. While we do not seek complete immunity, we would like to retain the present "good faith" exception.

Under §3121 of Title II of the legislation, we would like to expand the use of pen registers allowed to telephone companies to include use for investigative functions or for prevention of abuse of service. As I understood the conversation at the meeting, the Committee did not intend to prohibit the telephone companies from being able to investigate fraud or to prevent abusive or harassing calls.

We suggest that "use of" appearing at line 6 of §3123(b)(2) be deleted as being beyond the reasonable scope of assistance by a private party.

The discussion of §3123(d) centered around whether notice was required and whether the telephone companies would be required to give the notice. I believe that the consensus was that it should not be the telephone company's obligation to do so.

With respect to the limited immunity granted by §3128, the same thoughts as those contained in the discussion of §103 of the legislation apply. Moreover, since "emergency use" of a pen register is authorized under §3124, it would seem that the exception from liability should be extended to good faith reliance on a proper request under §3124.

We hope that our comments will be of benefit to you and other staff counsel. If we may be of further service, please let me know.

Yours very truly,

Hubert F. Owens

Hubert F. Owens

HFO:ls

C&P Telephone
1710 H Street, N.W.
Washington, D.C. 20006
Phone (202) 392-5127

Douglass J. McCollum
Attorney
Legal Department

October 22, 1985

Subcommittee on Courts, Civil
Liberties, and The Administration of Justice
Rayburn House Office Building
Washington, D.C. 20515

RE: H.R. 3378

In our meeting on October 10, 1985, I commented on the word "placement" in Section (h)(ii) (at p. 3 of the bill). I am concerned that "placement" may be construed narrowly to mean no more than a paper record showing the date, time, and originating and terminating numbers.

Such a limiting construction would adversely affect the investigations of toll fraud which are conducted by telephone company personnel. During these investigations, company personnel may record a limited portion of a fraudulent call. This has been a valuable tool in convicting people who defraud the telephone companies, and several courts have said that it is lawful under 18 U.S.C. §2511 for this limited recording to be made.

As you requested, set forth below are a few of the reported decisions supporting the recording by telephone company personnel of a fraudulent call. *United States v. Auler*, 539 F.2d 642 (7th Cir. 1976), *cert. denied*, 429 U.S. 1104 (1977); *United States v. Goldstein*, 532 F.2d 1305 (9th Cir.), *cert. denied sub nom*. *Roberts v. United States*, 429 U.S. 960 (1976); *United States v. Freeman*, 524 F.2d 337 (7th Cir. 1975), *cert. denied*, 424 U.S. 920 (1976); *United States v. Clegg*, 509 F.2d 605 (5th Cir. 1975); *United States v. Shah*, 371 F. Supp. 1170 (W.D.Pa. 1974).

Mr. David W. Beier, III, Esq.
Ms. Deborah Leavy, Esq.
October 22, 1985
Page Two

Should you have any further need for my assistance, please let me know.

Very truly yours,

Douglass J. McCollum

Douglass J. McCollum

DJM:bsr

Northwestern Bell

Warren G. Austin
General Attorney

Room 1430
1314 Douglas Street
Omaha, Nebraska 68102
(402)422-5606

September 30, 1985

U. S. House of Representatives
Committee on the Judiciary
Room 2137B - Rayburn House Office Bldg.
Washington, D. C. 20515

Re: "Electronic Communications Privacy Act of 1985"

Wayne Allcott, U S WEST Washington Office, suggested that I send to you some comments prior to our pending meeting at 10:30 a.m. on Friday, October 11.

First, let me say that I think that the bill is in reasonably good condition, from the standpoint of an operating telephone company. I look forward to meeting you and your staff, however, because I assume that there will be ongoing changes which may require some further communication by mail or telephone.

My comments refer to the discussion draft dated 12 September 1985, in the event that there were further changes prior to introduction.

On page 3, lines 21-23, provision (i) appears to be incomplete; I do not understand it as it is written. In the same vein, on page 21, lines 19-22, there is used the term "physical entry." There is no previous reference in Section 3125, however, to "physical entry." I suspect that that language was lifted from a previous section, such as on page 12, lines 9-12, without any preliminary material.

There are two exceptions for providers: page 3, beginning on line 24 through line 2 on page 4; and page 14, lines 9-13. I merely raise the question whether it would be helpful if there were language relating these two exceptions, i.e., calling attention to the two of them.

The provision which we are most concerned about is the matter of assistance in an emergency situation (page 21, lines 16-18). While the number of persons so authorized appears to be small, it puts the telephone company in the position of having to decide whether there is an emergency justifying assistance without a court order. Our concern is deepened by the fact that the exception to the recovery of civil damages, page 26, line 25 through line 2 on page 27, does not include good faith reliance in complying with Section 3125 (a) (2).

The communications common carrier or other provider should not be put in the position of assuming the risk of complying with the assertion of a law enforcement officer that such an emergency exists, only to find later in litigation that no such emergency did exist pursuant to the statute. While I am not quite sure how to correct the situation, if the provision is to remain, at a minimum there should be a good faith reliance exception. Perhaps Section 3128 (c) could be broadened to cover that situation.

I'll be happy to discuss these and any other items in the bill with you when we meet on October 11.

Yours very truly,

Warren Austin

Warren G. Austin
General Attorney

cc: Wayne Allcott

# ACLU PRIVACY AND TECHNOLOGY PROJECT
SEPTEMBER 1984

MEMORANDUM

TO: Conferees and Interested Persons

FROM: Jerry J. Berman and Marc Rotenberg

RE: New Forms of Communication: Are They Protected by Law? A Summary of the ACLU-PICA Privacy and Technology Consultation held on June 12, 1984

## Introduction

On June 12, 1984 the American Civil Liberties Union (ACLU) and the Public Interest Computer Association (PICA) held the first of a series of planned consultations in Washington D.C to explore privacy issues posed by the rapid development of new communications and computer technologies. The day-long conference, which brought together privacy and technology experts from the private sector and from congressional committees, was devoted to a discussion of new communications technologies and whether they are protected by current law from unauthorized interception. This Memorandum is a summary of the discussion. (See Appendix A for List of Attendees.)

## Overview of the Project

Before turning to topic of discussion, Jerry J. Berman, ACLU Legislative Counsel and Director of the ACLU Privacy and Technology Project, provided an overview of the Project and its goals:

The core assumption of the Project is that the revolution in new communications and computer technologies is undermining the fragile privacy protections embodied in law and that new laws and institutional arrangements are necessary. To cite a few examples:

--Government and business, for public policy and commercial purposes, increasingly use new computer technology to create data bases of personal information which can easily be accessed, shared, matched, merged and disseminated. The courts, however, have not recognized a right of privacy in records held by third parties. The Privacy Act of 1974, designed to give citizens some control over the use of this information and to require citizen consent before information collected for one purpose can be used for another, has proved ineffective because of technological change, legal interpretation, exemptions, and inadequate safeguards. The Privacy Act of 1974 protects "systems of records" but personal data can be amassed by accessing computer data bases which are increasingly not indexed as individual systems of records. The "Routine Use" exception in the Privacy Act has been interpreted to permit rather than inhibit "computer matching" of different data bases by the government to detect fraud and abuse. The technological capacity to bring together diverse data bases of personal information amounts to the creation of a de facto "National Data Center" despite considerable opposition to this concept only a decade ago.

--The new technology is creating new data bases of personal information that are unprotected by current law. For example, there are few state laws, and no federal law, protecting sensitive cable subscriber information, interactive cable functions, or consumer transactions via cable systems. The legal status of personal information in the possession of electronic mail companies is in doubt and the Right to Financial Privacy Act creates no right of privacy for electronic funds transfers.

--A decade ago, Congress barred the FBI's National Crime Information Center (NCIC) from engaging in "message switching" arrest records between states and completing a centralized bank of arrest records to serve the states because of fears that it would create a national police and give the FBI too much power over local law enforcement. There was also concern that too many arrest records (more than 50%) were inaccurate and incomplete and could adversely affect citizens' due process rights and employment opportunities. Today, the FBI is implementing a "decentralized" system which permits the states to hold their own records but advanced computer technology makes it possible for the FBI to compile any citizen's arrest record from one or several states in less than a minute. Little has been done to ensure that records exchanged are accurate or complete.

--A decade ago, the FBI used the NCIC system to keep track of anti-war and civil rights activists. Public revelation of the "Stop Index" brought it to a halt. But last year, the FBI added a similar index to the NCIC system to keep track of persons considered "dangerous" to Secret Service Protectees. without statutory authorization or legislated standards. The FBI is actively considering other indexes based on investigative and intelligence "non public record information" for inclusion in NCIC, including a terrorist index and organized crime "associates" list. Thus, the NCIC, a national computer network connected to 40,000 criminal justice agencies, is being transformed into a law enforcement intelligence and surveillance system.

The immediate purpose of the Project Consultations is to address these and other privacy issues to enhance our mutual understanding of the new technologies and the gaps in the law that have developed as a consequence of these new technologies. If a reform agenda is developed to address these gaps in the law, it should be based on a firm understanding of the changing technologies. Moreover, the technology may offer new means of protecting privacy, such as encryption of data bases or software design that limits access to sensitive data or ensures that incomplete records, such as state arrest records. are not transmitted unless updated and complete. For this reason, we thought it essential to bring together not only privacy experts but technical experts and users of the new technologies, both from the private and public sector for a series of consultations devoted to the issues we have identified and others which may be suggested by the participants.

In the long run, the goal of the ACLU Privacy and Technology Project is to develop a reform agenda to address these privacy/technology issues and a broad-based coalition to help us pursue that agenda. It is our hope that others attending these consultations will join us in these efforts. However, *it is not the purpose of the consultations to develop a "consensus" on what reforms make sense or to act as a working coalition. The Project will take no official positions and no participant will be required to endorse an ACLU or any other policy position discussed at the meetings.*

### Morning Session: New Technologies of Communication

Marc Rotenberg of the Public Interest Computer Association chaired the morning session which was devoted to a discussion of the development of new forms of communication technology. While reserving for the afternoon a detailed discussion of whether current law protects the "content" of communications carried by new technologies from unauthorized interception, Marc Rotenberg outlined the importance of the technology discussion for individual privacy. For example, he observed that we are increasingly communicating data using computers which emit signals in "digitized" form. Even phone conversations carried by wire are being converted into "digitized" signals for transmission and then reconverted into voice at the other end of the line. Yet the current federal wiretap statute, Title III of the Safe Streets Act, only protects against the unauthorized interception of "aural wire communications", meaning communications which may be overheard by ear. Since "digitized" signals are not "aural" communications, the content of these communications as well as the content of communications carried by other new forms of communications technology, may not be protected from government or private interception under current law.

To set boundaries around the technology discussion, Rotenberg stated that we would only concern ourselves today with the privacy protection of communications "in the stream" of communication, although cautioning that the distinction "in stream" is increasingly imprecise. (For example, a computer creates a "digitized" communication when you hit a computer keyboard and is logically "in stream" before it goes over a phone line and deserves privacy protection as does a message sent over a line and now in a computer or electronic mail box at the other end of the line waiting to be read by the sendee.)

To understand the diversity of new communications technologies, Marc Rotenberg first called on Steven Ornstein of the Computer Professionals for Social Responsibility to describe "Arpanet", one of the first and most sophisticated of the now burgeoning "computer networks" serving specialized constituencies. Developed with his assistance in the late 1960's to tie together universities and military installations, Arpanet, with a large number of terminals and a diversity of languages, was extremely complex. In fact, according to Ornstein, the complexity of the system enhanced the security of communications because of the extreme difficulty of decoding the multiple streams of bits of information carried over transmission lines. Decoding was even more difficult for anyone trying to tap signals in transmission between terminals because the transmission was broken into many small "packets" which resulted in a distortion of messages between terminals. Ornstein and others added that further security was and could be achieved by using sophisticated encryption, signal scrambling, and frequent changes in user IDs and passwords.

Later in the day, the group returned to the topic of "technology" as a solution to the privacy issue and a number of points were made that are relevant in the context of the above discussion. George Divida, an expert in cryptography and David Kahn, author of The Codebreakers, emphasized that encryption and other technical means can make communications systems more secure but that there was no "technological fix" at least with respect to protecting the content of communications against government intrusion. Both pointed out that the National Security Agency (NSA) --and therefore the government-- has the technical means to break sophisticated security systems and all but controls developments in the area of cryptography to ensure its ability to break codes. Others pointed out that the cost and complexity of sophisticated security systems are beyond the means of most citizens and that the consumer, whether business or private citizen, is more attracted by simplicity of operation than in security measures which complicate computer applications. Large companies might be a market for sophisticated measures to protect information from competitors but not the average citizen. And again, no measures can protect against a government agency determined to intercept or access the "contents" of communications carried by the new technologies.

Marc Rotenberg then asked William Caming of AT&T to describe other new communication technologies. Caming listed a number of new ways we are sending private communications previously carried by wire in "aural" form or even by the mails. Our voice communications are being translated into "digitized" form and then back into voice over telephone wires. We are sending messages formerly sent by first class mail by computer to other computers in "digitized" form over phone lines. Both voice and digitized messages are carried in part by wire but also in part by microwave transmission. A phone call at one end of the line may be answered by someone using a cordless phone at the other end of the line which can be overheard on an FM radio. A car phone or "cellular phone"is really a communication carried by designated radio frequencies. Fiber optics as a technology for communication is just ahead of us.

A general discussion of the new technologies of communication followed with the general emphasis on the point that because technology is changing so rapidly, it is counterproductive to focus concern on the means of communication rather than on protection of the content of communications.

## Afternoon Session: The State of the Law

At the beginning of the afternoon session, John Podesta, Minority Counsel to the Senate Judiciary Committee summarized a paper on the state of the wiretap law that he prepared, with the assistance of David Beier and Deborah Leavy of the House Judiciary Committee's Subcommittee on Courts, Civil Liberties, and the Administration of Justice, for participants at the consultation. (See Appendix B.)

John Podesta began by observing that the morning discussion was instructive for framing a discussion of the state of wiretap law in two essential ways. First, it confirmed that the technical means of communicating voice and data is changing rapidly. Second, the participants appeared to share a general consensus that establishing legal protection for particular forms of communication rather than the content of communications was counterproductive.

In fact, under the current wiretap law, the prohibition against unauthorized acquisition of the contents of communications is determined solely by the technical means used to communicate. Title III of the Safestreets Act of 1968 only prohibits the unauthorized "aural acquisition" of the contents of oral or wire communications. As intended by the drafters and as interpreted by the courts, only oral communications or wire communications which may be overheard (aural) are protected. "Digitized" voice or data communications carried by wire or other technical means are not covered by Title III.

The Foreign Intelligence Surveillance Act of 1978 (FISA) prohibits federal officials from engaging in the unauthorized acquisition of the contents of communications carried by new technical means because of its broad definition of "electronic surveillance" but the extent of the protection is unclear. In response to an inquiry by Senator Patrick Leahy, the Justice Department indicated that FISA may protect nonaural communications while carried by wire, cable or like communication, indicating that the interception of "digitized" communications may require a judicial warrant if carried by wire. (See Appendix C.)

However, if a communication is sent in part by wire and in part by microwave transmission or radio, a court order would be required under FISA only where "a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." Thus, the protection for new forms of communication depends on the Fourth Amendment, which leaves the scope of protection up in the air. The courts have not wrestled with many of the new forms of communication and whether a citizen has a reasonable expectation of privacy in communications carried by these new forms. When they have, the results have not been encouraging. For example, in the Jabarra case, a federal court of appeals held that NSA did not violate Jabarra's Fourth Amendment rights when it provided the "contents" of his communications to the FBI, communications which NSA intercepted by monitoring international microwave transmissions.

The best summary of the current law is the Justice Department Memorandum (Appendix C) which indicates that the government believes that protection for the content of communications depends on the means of communication rather than the content itself and that the privacy protection for new technical means is largely unsettled law. As the Memorandum notes: "In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions, such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious."

**Afternoon Discussion: Policy Options**

Following John Podesta's presentation of the congressional staff paper, the group engaged in a general discussion of different approaches to protecting the contents of communications carried by the new technologies. Here are some of the options presented:

1. Citizens should use technical means (encryption, passwords, etc) to protect their communications. As George Divida and David Kahn pointed out, however, there is no "technical fix" that would protect communications from government interception. (See Morning Discussion) As others argued, even if technical solutions were possible, citizens should have a reasonable expectation of privacy for their communications under the Constitution or laws of the United States.

2. We should engage in litigation to assert a reasonable expectation of privacy for communications carried by new technical means. For example, as Bill Caming pointed out, since "aural" acquisition of voice communications requires technical means to decode an electronic signal, we should not concede that "digitized" communications are outside the purview of the Safestreets Act. The extent of FISA protection also needs to be litigated in the courts. The general consensus was that litigation should be pursued but it would take years to sort out the law, even assuming that real cases developed. Moreover, given the current Supreme Court's approach to the Fourth Amendment, it is not at all clear that privacy would be enhanced by a series of test cases. In addition, none of these cases would resolve the issue of unauthorized access by private parties. FISA only applies to government officials and Title III protects against unauthorized acquisition of communications by private parties but only for limited forms of communications (aural acquisition of oral or wire communications).

3. Jerry Berman, John Podesta and others suggested that legislation could be drafted to change the focus of Title III to cover the content of communications regardless of the technical means employed. The term "aural" could be deleted to indicate that any unauthorized acquisition was prohibited. The words "in part by" wire could be added to cover wire-microwave or wire-radio communications. The group agreed that while such a bill may not solve all problems (e.g. what about when a communication is out of the stream) or may go too far (it would establish a broad prohibition on private citizens accessing computers even though they have no intent to engage in trespass or other criminal activity), it was a way to put the issue before the public and the Congress. As problems were identified, the statute could be refined.

4. David Beier and Deborah Leavy also argued that legislation should be introduced to focus attention on the issue and to start the process of updating clearly antiquated law. However, they believe the reform effort should be more inclusive to deal with other shortcomings of current law. They circulated a draft bill which would among other changes: (1) strike the word "aural" in Title III to protect the content of communications regardless of the technical means of communication, (2) add new "minimization procedures" for wiretaps and bugs, (3) establish a court order requirement for pen registers, (4) add a warrant requirement for video surveillance, and (5) limit the use of FISA taps to gather evidence for use in criminal prosecutions.

**Recent Developments**

Since the consultation in June 1984, the following developments have occurred:

1. In June, Congressman Robert Kastenmeier circulated for comment a bill drafted by his staff (David Beier

and Deborah Leavy) to address the gaps in the current wiretap laws.

2. On August 4 and 5, the Individual Rights and Responsibilities Section of the ABA held a Privacy Conference in Chicago. The group recommended that the IR&R section seek to place the ABA on record in support of a broad privacy law reform effort next year. Part of that agenda would be reform of the wiretap statutes to cover new communications technologies.

3. On August 7, the IR&R, Administrative Law, and Corporation, Banking and Business Law sections of the ABA presented a Privacy Program at the ABA convention. Senator Patrick Leahy delivered the keynote speech which focused on the need for new legal safeguards for the contents of communications carried by new communications technologies and announced that he would introduce legislation in the fall to deal with current gaps in the law.

4. A second Justice Department letter to Senator Leahy clarified the protection of new forms of communication but leaves many issues unresolved. (Appendix D)

## APPENDIX A

### ACLU-PICA Technology and Civil Liberties Project
### "Security of Digitized Information"
### June 12, 1984

### Conference Participants

David Beier, House Subcommittee Courts, Civil Liberties and Administrative Justice

Jerry Berman, American Civil Liberties Union

Nolan A. Bowie, The Aspen Institute

Bill Caming, AT&T

Richard Coughenour, Citibank N.A.

George Davida, University of Wisconsin

John Eiliff, Senate Select Committee on Intelligence

Lance Hoffman, George Washington University

David Kahn, Newsday

Deborah Leavy , House Subcommittee Courts, Civil Liberties and Administrative Process

Steve Metalitz, Senate Subcommittee Copyright, Patent and Trademark

Severo Ornstein, Computer Professionals for Social Responsibility

Paul D. Palermo, TRW

John Podesta, Senate Subcommittee Security and Terrorism

Eric Richards, Milbank, Tweed, Hadley, and McCloy

Marc Rotenberg, Public Interest Computer Association

John Shattuck, Harvard University Office of Community and Government Affairs

Randy Stratt, The Source

Karen Weickart, House Committee on Science and Technology

Fred W. Wiengarten, Office of Technology Assesment

Fred Wood, OTA Project on Information Technology

### OBSERVERS

David Burnham, The New York Times
Jim Dray, OTA
Charles Lamb, OTA
Pricilla Regan, OTA
Karen Menichelli, Benton Foundation

Appendix B

MEMORANDUM

TO: Jerry Berman, ACLU

FROM: John Podesta, Minority Counsel, Senate Judiciary Committee;
David Beier, Counsel, House Judiciary Committee;
Deborah Leavy, Counsel, House Judiciary Committee

RE: Focus Paper, Unauthorized Acquisition of Digital Communications

DATE: June 5, 1984

We are looking forward to meeting with you and the group you are assembling on June 12 to discuss the state of the law governing electronic surveillance. We think this meeting is important since the current law is in serious need of reform. And it is timely, since the current Administration is considering expansion of electronic surveillance techniques and the Congress is beginning its task of overseeing the statutes involved.

As part of its drive to halt the flow of critical military technology to the Soviet Union, the Department of Defense has created a task force to study appropriate mechanisms for intercepting the flow of computer software having military application. One option being considered by the task force is a program of massive electronic surveillance of transnational computer-to-computer communications. While this plan does not appear to be close to being operational, the Administration apparently is of the view that it can carry out such a plan without running afoul of the federal wiretap laws. (See Washington Post, May 6, 1984, attached.)

The above example points to the significant gap in the federal laws governing the unauthorized interception of electronic communications. This gap results, in large part, from our present communications revolution. We have witnessed over the last decade a blurring of computer and communications technologies -- or, perhaps more precisely, the integration of computer and communications technologies into networks which transmit information in a "digitized" form.

Today, vast amounts of data are transmitted between computers via wire and microwave radio transmission in a digital form. But the matter does not end with computer-to-computer communication. Increasingly, voice communications are converted from analog to digital form, transmitted via the telecommunications network, and then reconverted to an analog form at the other endpoint of the communication. Transmission of video information is beginning to follow this pattern, and will do so increasingly in the future.

The circumstances under which federal law proscribes the unauthorized interception of digital communications are extremely unclear. In 1968, when Congress enacted the federal wiretap law, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2510-2520 (Title III), it failed to cover acquisition of information in digital form. Title III covers only the "aural acquisition" of the contents of an oral or wire communication. The aural acquisition language of the statute has been interpreted by the Supreme Court to mean that to be covered by Title III, a communication must be intercepted in a form which is capable of being overheard. (See United States v. New York Telephone Company, 434 U.S. 159 (1977).) Apparently, this interpretation is consistent with the intent of the drafters of Title III. G. Robert Blakey, who was the principal staff counsel working on Title III, is quoted in the attached National Journal article as stating, "Did we intend to exclude machine-based data? Yes we did...Congress wasn't prepared to step into computer privacy, and that's the reason we put the work /"aural"/ in there." Evidently, those working on Title III did not anticipate the acquisition of voice information in the form of machine-based data.

Although not covered by Title III, nonaural interceptions by law enforcement personnel may be governed, in some cases, by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §1801-1811 (FISA). Recently, in response to an inquiry by Senator Leahy, the Department of Justice analyzed when FISA would require law enforcement personnel to obtain a court order before conducting a nonaural interception of an electronic communication. (A copy of the Department's analysis is attached.)

In brief, the Department is of the view that FISA imposes a court order or warrant requirement on law enforcement personnel who are intercepting a "wire communication" "while it is being carried by wire cable, or like communication." However, the requirement of a court order or warrant for the nonaural interception of a radio or microwave transmission only exists where "a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." Thus, the protection provided by FISA for the radio or microwave portion of a combined wire-radio transmission, is coextensive with the protection provided by the Fourth Amendment.

The Department goes on to note that:

> In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions, such as (whether there does or does not exist a reasonable expectation of privacy) are not always clear or obvious.

Therefore, the legal protections against unauthorized acquisition of digital communications are left largely to case-by-case determinations by the federal courts of whether there exists a reasonable expectation of privacy. The Court of Appeals decision in Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982), cert. denied, ___ U.S. ___ (1983) demonstrates that the government's technical ability to intercept and interpret electronic communications may be enough to defeat a person's reasonable expectation of privacy.

Data encryption may be the answer to some who wish to foil the unauthorized interception of a communication or to establish a more "reasonable" expectation of privacy. On the other hand, a person using encryption may be deemed to have a level of knowledge and sophistication high enough to create a presumption that person knew of the government's ability to acquire and decode the information. Thus, the reasonableness of the person's expectation of privacy is again called into question. Whatever the outcome of that debate, the cost of encryption is high enough as to be economically out of the reach of the ordinary citizen.

What this means is that the law may allow a vast amount of information transmitted partly by wire and partly by microwave to be acquired by government agents without a warrant or court order.

The restrictions on the private acquisition of this type of information are even fewer. Title III does not cover nonaural acquisitions. The Fourth Amendment has no effect. And since the activities prohibited by FISA require that the relevant electronic surveillance be carried out under color of law, even the minimal restrictions in FISA are largely inapplicable to the private sector. The only federal statute which may prohibit a nonaural acquisition of a radio or microwave transmission may be §605 of the Communications Act of 1934.

Section 605 provides, in part, that:

> No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.

There are statutory exceptions in this rule for radio transmissions intended for the use of the general public, ham radio operators, and CB operators.

On its face, §605 seems to prohibit unauthorized interception of a microwave transmission of a digital communication, where the party who intercepts the communication discloses the contents to a third party. However, courts have found that Congress intended Title III to be the exclusive remedy for unauthorized interception of communications in the telephone network. (See Watkins v. L.M. Barry & Co., 704 F.2d 577 (5th Cir. 1983) (private parties); U.S. v. Hall, 488 F.2d 193 (9th Cir. 1973) (law enforcement officers

Therefore, §605 provides protection only where the communication is a direct radio communication between sender and the intended receiver, and a disclosure to a third party results.

In particular circumstances, some protection against unauthorized acquisitions may be granted by the federal fraud statutes or by state enactments. But even if that is true, we think it is fair to conclude that the federal law governing electronic surveillance is clearly in need of updating.

To date, most of the public and congressional attention has focused on computer crime, featured prominently by media including movies and television, and superficially understood by legislators as a "problem" to be solved. Because no official governmental statistics are kept, most of the evidence offered about that "problem" is anecdotal. Several bills have been quickly drafted and introduced. However, proposals thus far have failed to address the fundamental policy questions which arise from the use of electronic means to achieve criminal purposes.

For example, currently pending in the House of Representatives is a computer crime bill, H.R. 5616, which criminalizes "time stealing" by federal employees, fails to protect privacy interests, and raises serious First Amendment problems. Yet despite all of these shortcomings,this legislation -- or another bill like it -- because of the popularity of the issue is likely to move ahead. We think that this example demonstrates the need for Congress to precede any legislative effort aimed at updating the electronic surveillance laws with an extensive inquiry into the nature and extent of the problem.

Now is the time to begin that process. Many questions, both technological and legal, have already been raised. (See the attached article by David Burnham.) Many more will certainly arise in the future. We believe that Congressman Kastenmeier's hearings in this area have begun to provide answers to some of these questions. As you know, Senator Mathias has agreed to Senator Leahy's request that hearings on this subject be held in the Senate, as well. The Office of Technology Assessment is also undertaking a study at the request of Congressman Kastenmeier and Senator Mathias to explore the topic of government information systems and privacy. We are hopeful that the future hearings and study will take a broad look at both federal wiretap and communication laws with a goal of more thoughtfully and fully protecting personal privacy from government and private intrusion.

As congressional staff participants in the June 12 meeting, we think the group of experts you are assembling can be extremely helpful at enumerating the problems we are facing and pointing us in the direction of legislative solutions. To that end, we would suggest the list of questions which follows as a starting point from which the group can begin its discussion.

Is the trend in the telecommunications system to transmit increasing amounts of information in a digital form?

Will this be true of data, voice, and video?

Does the technology exist to intercept digital communications transmitted by microwave and convert them into a readable form?

If the technology exists, is it currently available only to the government, or can private concerns acquire such technology?

Are there practical, non-governmental solutions, such as data encryption, available to the person who seeks to defeat the unauthorized acquisition of a digital communication?

Was Title III intended to cover voice communications which had been converted to a "digitized" form for transmission?

Did Congress intend that Title III be the sole remedy available to a party for the unauthorized acquisition of a communication in the telephone network?

Should Congress establish different standards of privacy protection for different means of human communication? Should voice communication be granted greater privacy protection than written communication?

Can Congress provide a definition of "reasonable expectation of privacy," or must that be left to a case-by-case court determination?

What law enforcement problems are created by eliminating the reasonable expectation of privacy proviso from the FISA electronic surveillance definition governing microwave transmissions of communications?

If Congress undertakes a reform of the electronic surveillance laws, should it concentrate on amendments to Title III and FISA, or must it also amend §605 of the Communications Act?

What restrictions exist on the government's collection of information being transmitted by open access electronic mail systems?

Should video surveillance be permitted under any circumstances, and if so, what kinds of restrictions should be placed on video surveillance to avoid running afoul of the Fourth Amendment prohibition against general searches?

Should Congress consider creating a permanent administrative body or commission to study the privacy problems generated by the new technologies?

Would the House and Senate be well-advised to create their own select committees to review privacy problems?

Centel Corporation

CENTEL

1140 Connecticut Avenue, N.W.
Suite [illegible]
Washington, D.C. 20036
Telephone 202 833 8700

Martin T. McCue
Director of
Government Relations

July 17, 1985

The Honorable Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties
and the Administration of Justice
Committee on the Judiciary
2137 Rayburn House Office Building
Washington, D. C. 20515

Dear Mr. Kastenmeier:

I appreciate your kind letter of June 17, 1985 concerning the preparation of the "Communications Privacy Act of 1985" (also titled the "Electronic Surveillance Act of 1985"). I also appreciate your request for comments.

I am sending this letter to provide you with both comments and suggestions concerning the draft bill you enclosed. These comments are being provided by me as an individual who has dealt at some length with Title III of the Omnibus Crime Control Act of 1968, and not on behalf of my employer, Centel Corporation, although by necessity I will explain a number of points below in the context of events and procedures involving Centel.

To begin, I note that the bill does not appear to pursue a particular philosophy. That is, it appears to be an objective attempt to close loopholes in the law to make its application current and consistent. I believe this is very important. It is important, especially in this area, to prevent court decisions on motions to suppress that might be based solely on the law's failure to anticipate new technologies and engineering applications. Stated another way, the draft does not attempt to either expand the use of wiretaps or to eliminate them as a law enforcement option. I also note an intention to unify the underlying principles that apply across the general search and seizure area. I consider these goals laudatory and I believe that reform would be constructive.

Your goals with respect to the draft bill are significant, since any comment I might make on the draft bill would normally be made partially in response to those goals. In these comments, I am assuming that the revisions are to be transparent to political considerations. This would appear to be the only way in which the subcommittee could realistically expect to obtain the needed revisions.

We are in a good and somewhat unique time period. There is a sufficient body of case law which has made most of the necessary changes fairly obvious, yet the emerging technologies have not reached a point where the loopholes in the law are an imminent threat to the law's usefulness as a proper law enforcement tool. This "window" may not last too long.

The following analysis is broken into three parts. First, I am providing my own current view of the law. Second, I am providing a description of some of my experiences in this area to illustrate problems that I believe exist. Third, I am providing a line-by-line series of suggestions on language modifications that might be of assistance to your subcommittee. In general, however, I found the bill to be well-drafted, with most of my suggestions based upon items you might not have anticipated.

I. The Law. Chapter 119 and, to a lesser degree, Chapter 205 of Title 18 of the U.S. Code contain the bulk of the statutory law involving the interception of communications and the balancing between privacy rights and legitimate governmental intrusions. Since the provisions of Chapter 119 were passed, they have become a popular site for litigation. However, the benefit of this high level of litigation to date has been a correspondingly high level of certainty that certain procedures are appropriate and certain procedures are not. Thus, in most routine wiretap situations, there is now a fairly bright line of established procedure which, when followed, will rarely result in judicial suppression of evidence, but which, when deviated from, could jeopardize entire investigations. Investigations involving Chapter 119 orders usually involve large investments of time and money, and thus there is more of an incentive than in a comparable search warrant case to comply strictly with the statute, lest an error negate all prior investigative work.

I note this to point out the fact that, with only a few exceptions, there is a pretty reliable body of case law on procedure, as opposed to what types of communications the law itself should apply to. Thus, as a random sample of issues which could have been more contentious but are now fairly settled, we have the following: a state law can be more restrictive but not more lenient toward law enforcement officers (U.S. v. Horton, 601 F.2d 319, cert. den. 444 U.S. 937 (1979)); prior voluntary consent of one party eliminates the warrant requirement entirely (U.S. v. Howell, 664 F.2d 101 (1981)); only certain enumerated or described offenses will justify an order (U.S. v. Webster, 472 F.Supp. 586 (1979)); a particular authorizing official need not explain his or her reasons for authorization or even remain in office at the time of an interception (U.S. v. Martinez, 588 F.2d 1227 (1978); U.S. v. Wyder, 674 F.2d 224 (1982)). Other types of specific litigated issues include: that specific additional authorizations for covert entry should be, but need not be included in a court order (compare Dalia v. U.S., 60 L.Ed. 177 (1979) with U.S. v. Licavoli, 604 F.2d 613, cert. den. 64 L.Ed 2d 787 (1979)); that evidence received may justify an entirely different criminal prosecution (U.S. v. Kerr, 711 F.2d 149 (1983)) and that an application may contain numerous errors, so long as probable cause still exists (U.S. v. DePalma, 461 F.Supp. 500 (1978)). So long as a governmental agency stays in the mainstream, it is likely to avoid suppression of evidence or other sanctions.

(There are a few procedural items that would be clarified by your bill. Thus, the question of whether "targets" of the interception be named in an application or order is resolved by some case law in the negative (U.S. v. DePalma, Id.), but would be modified in your bill. Also, your bill defines a new procedure for pen registers and for tracing calls.)

The questions of the applicability of the law are more problematic. Interpretations about the application of the law have not been consistent.

Opinions in cases since the adoption of Chapter 119 have stated, for example, that while an interception by a motel switchboard operator involves a "wire communication", an interception within a private computer "spy" system even before a signal reaches the public telephone network is not. Compare U.S. v. Axselle, 604 F.2d 1330 (1979) with U.S. v. Seidlitz, 589 F.2d (1978), cert. den. 441 U.S. 922. One of these cases is probably wrong, since the Axselle case involved a system which, in today's environment, would be the equivalent of a private, fully-independent electronic PAEX system that can handle calls to and from extensions internally and not touch the public telephone network except for outgoing and incoming calls. Indeed, the convergence of computers and communications has resulted in these motel switchboard operators being made almost completely obsolete by PABX telephone systems. Those systems become identical to the system in U.S. v. Seidlitz for purposes of Chapter 119.

Likewise, other opinions have indicated that Chapter 119 either does not apply to any of the following situations, or casts varying degrees of doubt upon its applicability:

a) Television surveillance. Video, as opposed to audio interception, is not governed by Title III. (U.S. v. Torres, 36 Crim. Law Reporter 2301 (1984). See also Cox Cable Cleveland Area Inc. v. King, 582 F. Supp. 376 (1983)).

b) Cordless telephone interceptions. Use of an AM radio to tune in on cordless telephone calls is not "wire or oral conversation". State v. DeLaurier, 37 Crim. Law Reporter 2004 (1985). But see State v. Howard, 235

Kan. 236 (1984) (cordless telephone carries "oral communications")).

c) Warrantless installation of a beeper device, even within a residence. Beepers do not intercept contents of communications. State v. Hendricks, 258 SE 2d 872 (N.C. App., 1979). Note that a beeper to track and locate items within a residence may require a warrant, but the case never discusses Title III issues. See discussion in U.S. v. Karo, 51 LW 5102 (1984).

d) Cellular mobile telephones. Discussion in U.S. v. Knotts, 460 U.S. 276 (1983), could be read broadly enough to imply that augmentation of sensory facilities using science and technology to further limit an already-lessened expectation of privacy in a moving auto allows certain types of interceptions. The better view is probably to the contrary, and there are a number of cases that discuss the "augmentation" issue as one involving the expectation of privacy. Also, State v. DeLaurier, above at b), could be relied upon where a cellular call is intercepted directly rather than while going through telephone company wires.

e) Data transmission. While there may be no reported cases yet, data transmission is not an "oral communication", and in many cases may not be a "wire communication." (Note an article in New York Times, December, 1983, to this effect, and recent Congressional concerns over unauthorized computer access.) U.S. v. Seidlitz, discussed above, really involves the theft of software over telephone lines, and some of the discussion implies that data interception would be covered by Chapter 119.

f) Other situations. Cases exist that also discuss the applicability to ham radio or point-to-point radio transmissions (U.S. v. Rose, 669 F.2d 23 (1982): interception permitted on other grounds); radiotelephones (U.S. v. Hall, 488 F.2d 193 (1973): interception permitted); non-telephonic conversations heard through a telephone that is left off-hook , (People v. Basilicato, 36 Crim. Law Reporter 2267 (1984): use prohibited);

These cases do not even touch more routine interceptions, some of which have been validated by the U.S. Supreme Court. Pen registers have been explicitly permitted without either a wiretap order or warrant because there was no expectation of privacy recognized. Smith v. Maryland 442 U.S. 735 (1979). (There is some dissent within the communications industry about the assumptions in Smith, especially for certain classes of customers who pay for a greater degree of privacy.)

A second area for similar types of interceptions involves trap- or tracing-devices. These are widely used, under many different legal standards, but there is little explicit case law on their legitimacy. Smith v. Maryland does not clearly cover the facts, and the "expectation of privacy" analysis is not identical. One reported case notes that Chapter 119 doesn't apply to traces, since there is no interception or "aural acquisition". (Michigan Bell v. U.S., 565 F.2d 385 (1977)). U.S. v. Seidlitz, discussed above, also validated a series of broad, sophisticated traces.

In addition, most states have unique statutory provisions that involve trap- and trace-devices, rendering the law quite varied. Lastly, a number of states do not permit interceptions with the consent of only one party to a call.

II. My Own Experience. My own experience with these types of situations breaks down into two discreet areas- one involving actual wiretap orders and one involving orders regarding trap- and trace- devices. They must be evaluated independently. As a counsel for Centel's telephone companies, I had routinely reviewed both types of orders to ensure that they complied with applicable laws, and I did so to eliminate any civil exposure for Centel. The law provides an affirmative defense for common carriers acting in good faith reliance upon an order. 18 USC 2520. Centel policy is that its attorneys must review the facial validity of each order under applicable law to ensure that its good faith remains "reasonable." See Jacobson v. Rose, 592 F.2d 515 (1978), cert. den. 442 U.S. 930. In a few cases, this has gone so far as to justify a return telephone call to an issuing federal judge to confirm his actual execution of an order. We have been careful because we know of a number of civil suits against common carriers.

Centel has generally been very protective of the privacy of its customers' communications. It has an internal directive that is arguably more restrictive than the case law requires in some areas, and it has been revised as situations demand or as the law changes. (A copy is attached of the current, slightly outdated directive, for which a review has been underway for some time. Also attached is an early draft of a replacement.) Centel's involvement in one matter in Nevada in the early 1970's led to an amendment in Chapter 119 involving common carriers.

As I noted above, the procedures for wiretap orders generally have become very structured and the orders, when presented, have already been the object of much review and scrutiny. It also could be that, because of the care required by Centel's general counsel, many law enforcement officials we worked with became more careful themselves. At times, we reviewed orders beforehand and told the officials what had to be included for Centel to comply.

To my everlasting surprise, it has been the other area, involving the tracing of more common events, that seems to present the most problems. These events are normally obscene or harassing telephone calls. While I believe there are actually fewer wiretap orders than most people might expect, telephone call tracing is fairly common. You should be aware of this as you attempt to decide the procedures that will be adopted. Also, tracing in many cases is identical to internal activities undertaken by telephone companies to pinpoint network transmission problems.

I believe that the administrative problems arose because of the unclear statutory law, the often-emergent nature of the requests and the fact that a few local law enforcement agents were impatient to act, even without an order, because they had a suspect and generally knew the victim. These activities also tended to become repetitive in certain small communities, and we found that we often dealt with police or prosecutors only in certain of the areas we served. Here, too, we suggested to law enforcement officials certain safeguards which we expected, including a "John Doe" type proceeding where a caller was unknown. We believe, however, that other common carriers do not follow identical procedures, and we have had feedback that we are more demanding than some others. We have recently considered more lenient guidelines in light of the *Smith v. Maryland* case, but I note that your draft bill is not too much different than our existing policy in many respects. (I am providing a significantly different definition of "tracer" than your bill now includes in my comments.)

To my knowledge, with any wiretap order, we have always declined to enter a premises with law enforcement officials when that entry had to be covert, although under the law, we have been required in certain orders to stand by and render instructive technical assistance by radio or telephone. (With tracing devices, no entry is required. An adjustment in the central office permits a circuit to stay open or be pinpointed so that the number of the caller and called party can be identified. The particular activity depends upon the technology used in the telephone company's central office switch. Interception of conversation does not occur in those cases. With traces, the cooperation of a victim is needed to match the time of the call that is traced by the telephone company with the time of the call identified as offensive or harassing by the victim.)

It also has become our policy to recognize practical impacts. Thus, where there is an emergency, such as in a 911 call, hostage situation or house fire, we believe it is justified to presume consent. We find it impossible to conclude that a person whose line is involved in such a situation would not consent to tracing or other types of line identification.

All in all, these experiences have led to some of the suggestions made below.

III. *Suggested Changes*. Before leading into line-by-line comments or suggested changes, I would suggest a few conceptual items for the subcommittee to address, based upon the cases discussed above. In most cases, these would not require legislation, and could be handled in the legislative history or by colloquy if the subcommittee determined that a policy decision was appropriate.

First, you should preempt the states on procedural requirements that involve traps, traces and pen registers to the same extent as is done for wiretaps in Chapter 119. Thus, state laws could be more restrictive, but not less so. This would aid in the coordination of these laws immeasurably.

Second, you should consider a cross-reference or separate codification of all federal privacy statutes involving telecommunications, including Section 605 of the Communications Act and the section of the recently-enacted Cable Communications Policy Act of 1984. There is more of a convergence today between tracing and such things as theft of service in the cable television area. See Cox Cable Cleveland Area Inc. v. King, 582 F.Supp. 376 (N.D. Ohio, 1983). Your bill begins to do this by discussing computer intrusions and related activities.

Third, you should determine in a statute whether "severance" of wiretap orders should be permitted. More and more cases now permit severance of search warrants, allowing some portions to be executed, and others rendered invalid. See Commonwealth v. Lett, 36 Crim. Law Report 2138 (1984). The law should be consistent, whether it is a search warrant or an order under Chapter 119 that is involved.

Fourth, the recent cases of U.S. v. Leon, 52 LW 5155 (1984) and Massachusetts v. Sheppard, 52 LW 5177 (1984) could pose problems in this area. In each of these cases, the Supreme Court upheld evidence gained from an illegal search warrant where an officer acted in reasonable reliance on the warrant. I do not believe these cases should be allowed to be utilized in the electronic surveillance area although, again, there is a benefit in consistency. I believe the greater significance of a Chapter 119 order justifies no exceptions. Also, there must continue to be a very clear, detached judicial role in authorizing and setting limits for wiretaps.

Fifth, the subcommittee should look at the application of two other doctrines to the electronic surveillance area- the "inevitable discovery" rule that allows evidence to be used if it would have been discovered anyway (See Nix v. Williams, 52 LW 4732 (1984)), and also the "open fields" doctrine, in light of the permissable "enhancements to science and technology" language in U.S. v, Knotts, 460 US 276 (1983), mentioned above. In the latter case, three judges dissented specifically to the "enhancements" language in light of other cases, and such a test would have few limits in the electronic surveillance area. There is a clear conflict between enhanced eavesdropping under the "open fields" doctrine and a subjective expectation of privacy. See, e.g., U.S. v. Agapito, 620 F.2d 324 (1980), and its progeny. While the Fourth Amendment is claimed to protect conversations that can't be heard except by electronic enhancement, the Supreme Court language may undercut this principle. Also, it is my understanding that there is another 1974 case in the environmental area which has permitted the use of sophisticated electronic equipment to test air pollution, and justified its use in court under the "open fields" doctrine.

The specific comments on your draft follow as an attachment, and a markup is also attached for reference. I hope that they will be of use to you in your work. You may feel free to redistribute this letter if you so desire. Thank you again for the opportunity to be of assistance.

Very truly yours,

Martin T McCue

Martin T. McCue

Enclosures

MTMC:lca

cc: Karl Berolzheimer
    Deborah Leavy

"Electronic Surveillance Act of 1985"
Discussion Draft MDB416 (4 June 1985)

| Page | Line | Modification (and Reason) |
|---|---|---|
| 2 | 24 | Delete "intends". Insert "does not intend". |
| 2 | 25 | Delete "accessed by". Insert "unavailable to". (Alternative: insert "withheld from".)<br>Reason: Suggested language tracks the current case law. Technically, the test is whether privacy is intended, not whether public access is intended. There are significant differences. |
| 3 | 2 | Delete "by any station". |
| 3 | 4 | Delete "in distress". Insert "who (or whose occupants) might be deemed to be in such distress that consent to interception could reasonably be inferred to avoid death or serious bodily injury,".<br>Reason: Suggested language covers the preexisting distress situations, but also accommodates newer situations where consent to interception should be inferred. |
| 4 | 4 | Clarify (in legislative history) that "targets" refer to individuals, and consider policy issues related to standing for later motions to suppress. |
| 4 | 9 | Delete "tracers". Insert "devices for trapping circuits or tracing calls, temporary programming of the switches of a telephone company or other common carrier"<br>Reason: The suggested language is more precise in describing what is actually done. "Tracers" is not a universally accepted word. This will reappear throughout this commentary. |
| 4 | 15 | Delete "any further".<br>Reason: Including these words implies that these technologies will have been used in every case already. That is not always so. The goal should be to show why they cannot be used from the present point forward. |

| Page | Line | Modification (and Reason |
|---|---|---|
| 4 | 19-20 | Query whether language "mobile interception device" covers all cases, such as those involving car or drum. |
| 4 | 25 | Delete "wire". Insert "electronic".<br>Reason: Consistency with your earlier language. |
| 5 | 4 | Insert "No common carrier or its agent shall be compelled to participate in such physical entry."<br>Reason: Law enforcement officers should be the only persons to enter premises whenever possible. Common carriers are in different position from landlords, owners, etc. They have no right to enter, however contingent. |
| 5 | 8 | Query whether there should be a minimum duration of authorization under an order before this section comes into play. |
| 5 | 17 | Delete "or". Insert "and shall suspend or terminate interception if any such report"<br>Reason: Fourth Amendment probably doesn't give a judge any discretion when probable cause ceases to exist. |
| 6 | 9 | Delete "made". Insert "signed".<br>Reason: This makes it easier to judge application of the new law. |
| 6 | 19 | Delete "wire". Insert "electronic".<br>Reason: Coordination with remainder of bill. |
| 7 | 11 | (Clarify term "film", insofar as it might relate to motion pictures or still photography.) |
| 7 | 12-14 | Clarify "public location". Video surveillance may be lawful though made from a private location, so long as one has the right to be there. Possible alternative: insert "place where a person engaging in such surveillance is lawfully present". Also, it is not clear that the one-party consent rule has any application to video surveillance except as it might involve audio recording of a conversation. The fact of presence at the conversation would seem to be consent to any video |

| Page | Line | Modification (and Reason |
|---|---|---|
| | | recording but without sound. |
| 8 | 8 | Delete "tracer". Insert more accurate wording. |
| 8 | 11 | Delete "$250,000". Insert "$10,000".<br>Reason: This is just a suggestion. As a practical matter, the original sum is far too high given the nature of the activity. |
| 8 | 12 | Delete "five". Insert "one".<br>Reason: See just above. |
| 8 | 13 | Insert new subsection (c): "This subsection shall not apply to common carriers when the sole purpose of such activity is to aid the common carrier in the operation, maintenance and testing of communications facilities."<br>Reason: The activities used by telephone companies to test for network problems are often identical to that used in tracing calls. The idea is to keep the circuit open or identified until it can be addressed. |
| 9 | 22 | Delete ".". Insert ", including the existence of consent, or where appropriate, circumstances where consent may be implied."<br>Reason: This addition is particularly useful in this context and should be considered fully lawful and appropriate when it will be reviewed by a judicial officer. |
| 9 | 23 | Substitute for "tracer". |
| 10 | 3 | Substitute for "tracer". |
| 10 | 7 | Substitute for "tracer". |
| 10 | 14 | Insert after "person" "whose calls are". |
| 10 | 15 | Substitute for "tracer". |
| 10 | 20 | Substitute for "tracer". |
| 10 | 24 | Delete ";". Insert "including a finding as to the existence of express or implied consent." (Also, substitute for "tracer".) |

| Page | Line | Modification (and Reason |
|---|---|---|
| 11 | 2 | Substitute for "tracer". |
| 11 | 4 | Substitute for "tracer". |
| 11 | 9 | Delete ".". Insert ", but no order shall require a common carrier or its agent to enter premises to install, maintain or remove a pen register." |
| 11 | 12 | Substitute for "tracer". |
| 12 | 21 | Substitute for "tracer". |
| 12 | 24 | Because of the lesser privacy interests here, it may be worthwhile to allow more persons than the Attorney General alone to designate an officer to install and use a pen register or (tracer) in an emergency. See discussion above on consent. The fact that this is in the bill at all indicates subcommittee acknowledgement of a diminished expectation of privacy. |
| 13 | 4 | Insert "involving" after "exists". |
| 13 | 8 | Delete "or". |
| 13 | 10 | After ";" insert "or". Add "(IV) express or implied consent to utilize a pen register or (tracer) by a party to the situation". |
| 13 | 13 | Substitute for "tracer". |
| 13 | 18 | Substitute for "tracer". |
| 13 | 20 | Substitute for "tracer". |
| 13 | 23 | Substitute for "tracer". |
| 13 | 25 | Substitute for "tracer". |
| 14 | 1 | Substitute for "tracer". |
| 14 | 4 | Insert additionally the description used for tracer after "register".<br>Reason: A common carrier is the most likely entity to install or operate a tracing device, and its assistance is necessary. Such assistance is less necessary for pen registers. |

| Page | Line | Modification (and Reason |
|---|---|---|
| 14 | 7 | After "register", insert description used for tracer. |
| 14 | 11 | After "register", insert description used for tracer. |
| 14 | 18 | After "register", insert description used for tracer. |
| 14 | 18 | Insert new subsection (b), renumbering existing subsections (b) and (c) as (c) and (d), respectively. "No common carrier shall be compelled to enter the premises of a party whose line is to be the subject of a pen register or trace." |
| 15 | 11 | Substitute description used for "tracer". |
| 16 | 8 | Substitute description used for "tracer". |
| 16 | 12 | After "register", insert description used for "tracer". |
| 16 | 20 | Substitute description used for "tracer". |
| 17 to 19 | 6<br>5 | I would suggest that the subcommittee carefully consider the nature of the reporting obligation here, since the use of tracers is so common. It would be better to require reports only for pen registers, since the overwhelming majority of traces are made with the express consent of the party who has subscribed to the service. |
| 19 | 18 | Substitute language used for "tracers". |
| 20 | 2 | Assuming that the word "tracer" is retained, I would suggest that it be defined in a different way: "the term "tracer" means an electronic or mechanical device, arrangement or program which permits the identification of a telephone or line from which a telephone call or other communication originates". |
| 20 | 13 | Substitute new description used for "tracer". |
| 20 | 17 | See discussion in text on this general issue. The sections of Title IV running in the draft bill from pages 20 to 30 are probably best addressed by the providers and users of these |

| Page | Line | Modification (and Reason |
|---|---|---|
| | | services, and the language should be conformed with that in related "theft of service" or "unauthorized access" statutes. |

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON OFFICE

600 Pennsylvania Ave., SE
Suite 301
Washington, DC 20003
(202) 544 1681

National Headquarters
132 West 43rd Street
New York, NY 10036
(212) 944 9800

Norman Dorsen
PRESIDENT

Ira Glasser
EXECUTIVE DIRECTOR

Eleanor Holmes Norton
CHAIR
NATIONAL ADVISORY COUNCIL

June 26, 1985

Rep. Robert W. Kastenmeier
Chairman
Subcommittee on Courts,
Civil Liberties and the Administration
of Justice
U.S. House of Representatives
Washington, D.C. 20515

Dear ~~Representative~~ Bob Kastenmeier

We want to thank you for this opportunity to comment on the June 4, 1985 draft of your "Electronic Surveillance Act of 1985." As you know, the American Civil Liberties Union strongly supports congressional efforts to restore and enhance privacy rights threatened by the development and use of new communications and computer technologies. We applaud your recognition of the significance of these issues and your willingness to play a leadership role in fashioning reforms.

During the last year and a half, we have sponsored and coordinated several consultations on privacy issues posed by new computer and communications technologies which are addressed in your legislation. In addition to experts from your staff and other congressional offices, the consultations have been attended by a wide spectrum of persons representing public interest and business organizations as well as persons expert in new technologies. Out of these consultations a consensus has emerged that new technologies have rendered current statutory privacy protections ineffective and in need of reform. While we have not asked participants to take positions on particular bills, we believe that most of the participants would endorse many of the provisions of the draft bill and would work for their enactment.

The American Civil Liberties Union is strongly supportive of the privacy reforms in your draft legislation. Below, we comment generally on why we support each provision and offer suggested changes or amendments which we believe should be included in the legislation. Later, we would like to discuss with you whether the legislation should be considered as a package or as several bills. This may turn on whether the draft addresses most of the Administration's major objections to last year's bill, H.R. 6343.

We believe you have done so without undercutting significant privacy reforms. However, their response to the new bill may suggest the need for several bills rather than one.

## Title I. Title III Amendments

### Section 101. Electronic Data Communications

At our consultation in June 1984, a strong consensus emerged that Title III does not protect "data" communications and should be amended to protect data as well as voice communications. The new definition of "Electronic Communication" makes the intent of this section to protect such communications clear. We note that the Justice Department did not appear to object to this reform in its commentary on last year's bill.

We think the addition of section 101 (g) is of particular importance, for it is necessary to draw a line between such communications (e.g. many electronic bulletin boards) and communications which are intended to be private. However, drawing this line is difficult, and we feel that more thought should go into refining this important exception to the rule. At an ABA Privacy Conference in Chicago on June 21-23, 1985, some bulletin board operators' descriptions of their systems pointed out the difficulty of drawing the line between "public" and "private" communications. Many electronic bulletin boards are opened to any who wish to log on. and the operators are interested in creating a "public forum." At the same time, the operators feel that they have a right to exercise some control over the bulletin board, and because the bulletin boards are their "creation", that they are somewhat private. They would like to have the First Amendment protections of a public forum, and yet have privacy protection against government intrusion (not unlike political groups who do not want their public meetings infiltrated by government investigative agencies without cause). We argued that they might not be able to have it both ways.

We suggest that one way to draw the line between "public" and "private" communications would be to require some form of access code to be employed by those who want privacy. This would also avoid the creation of a rather sweeping crime for "computer hacking" since private unauthorized interceptions of data communications would also be criminalized by changing the scope of Title III interceptions. Unless "hackers" intentionally or knowingly overcome an access code, they should not be criminally liable for merely dialing up a system.

### Section 103-105.

We support these sections designed to give some substantive meaning to the "least intrusive means" test under Title III both for wiretapping and physical entry. We believe you have answered the major objections of the Justice Department to last year's drafting of these sections and omitted changes which might have endangered the chances for some reforms to be accomplished because of Justice Department opposition.

## Title II. Video Surveillance

We strongly endorse a judicial warrant requirement for video surveillance. We believe the government can not object to this provision in light of the Torres holding, which this section codifies, particularly since Judge Posner implored the Congress to develop clear rules for such surveillances. The one-party consent rule change in this year's draft is unfortunate, but necessary to remove serious Administration opposition to statutory regulation of this highly intrusive technique.

## Title III. Pen Registers and Tracers

We believe it is important to establish a court order requirement for pen registers and tracers. With respect to the former, we do not agree with the majority opinion and holding in Smith v. Maryland, 442 U.S. 735 (1979), that a record of phone call numbers does not reveal the contents of communications or that citizens have no expectation of privacy in a record of who they call because the phone company keeps records. Why would investigative agencies seek such records if they did not reveal information about the target? A record of phone numbers can reveal a person's political affiliations, network of associates, shopping habits, and more. Recent concern that a proposed federal government audit of phone calls placed by federal employees could detect "whistleblowers" as well as "abuses", particularly if local calls are also monitored, applies to pen registers as well.

With respect to tracers, the Supreme Court has recently held that tracers can intrude on a person's reasonable expectation of privacy in certain circumstances. United States v. Karo, 104 S.Ct. 3296 (1984).

We do not believe the court order requirements set forth in the draft bill pose a significant burden on the government. The current practice is to obtain a court order for pen registers and Karo requires that the government consider obtaining a search warrant in using tracers. The draft bill essentially codifies the practice and establishes a minimum standard sufficient to ensure that these techniques are used for appropriate and legitimate law enforcement purposes.

## Title IV. Electronic Communication Privacy

At an ACLU conference in January of this year, we focused on whether or not current law protects the privacy of electronic mail. The conferees agreed that current law does not provide clear or adequate protection. Because "data" communications are not protected under Title III, electronic mail may be intercepted without a warrant when it is being carried over the phone lines. The government could also obtain electronic mail from the service providers without a search warrant. (See Appendix for Conference Summary)

We believe electronic mail deserves similar protection to first class mail and private phone conversations. The draft bill would accomplish this by amending Title III to cover data communications, by establishing court order and search warrant requirements for government access to provider records or e-mail held by providers, and by making it a crime for private parties to gain unauthorized access to electronic mail.

We suggest three changes in the draft bill at this time:

First, civil suits for unauthorized access to electronic mail by government agencies should be against the United States. Our experience with FTCA amendments convinces us that personal liability will lead to Administration opposition to the proposed remedy.

Second, there must be a civil remedy against an electronic mail company which discloses records without authorization, similar to the remedy proposed in (c)(1) of section 702.

Third, if the government obtains a search warrant, a delayed notice provision must be added similar to the notice requirement for wiretaps. While mail statutes do not provide for delayed notice, a target of surveillance has constructive notice when the mail does not arrive. With respect to electronic mail, it would be possible for the government to obtain a copy of messages without the sender or addressee knowing of the fact. To test the legality of the surveillance, a notice provision needs to be included.

Title V. Computer Crime

As you know, we strongly support efforts to amend the section of the computer crime statute enacted last year that makes it a crime for a government employee with authorized access to a government computer to make an unauthorized disclosure of any information in the computer. On its face, this is a sweeping secrecy statute applicable to all information in government data banks. The amendment you set forth in Section 501 (2) would narrow the statute considerably. We hope you will consider offering this section as an amendment to computer crime legislation now pending before the House Judiciary Subcommittee on Crime.

We have no civil liberties objections to establishing federal penalties for various computer-related crimes. We do have questions about what computer crimes should come within federal jurisdiction. H.R. 5616 required a loss of $5,000 to establish some demarcation between federal authority and state police powers. This may be unsatisfactory. Your computer crime proposals turn on whether interstate commerce is affected. This is, of course, quite broad. Another possibility is whether the computer operates in interstate commerce or the crime occurs across state lines (e.g. computer hacker in state A steals funds from a computer in state B). It is just this sort of case which is difficult to reach under a state computer crime statute. State A may not want to prosecute because the loss occurs in state B. State B may have difficulty acting against the hacker because he or she resides in state A.

Summary

Again, we applaud your leadership role in seeking changes in law to protect privacy in the face of new technologies. If we can be of further assistance, please do not hesitate to contact us. We are anxious to see this legislation introduced and will work with you for its passage.

Warm Regards,

Jerry J. Berman
Legislative Counsel

ACLU PRIVACY AND TECHNOLOGY PROJECT
JUNE 1985

**MEMORANDUM**

TO: Conferees and Interested Persons

FROM: ACLU Project Staff

RE: Privacy and the 99th Congress and Protecting Electronic Mail. A Summary of the ACLU-Public Interest Computer Association Consultation on January 29, 1985

**Introduction:**

On January 29, 1985, the American Civil Liberties Union Privacy and Technology Project (ACLU Project) and the Public Interest Computer Association (PICA) held the second in a series of consultations in Washington. D.C. to explore privacy issues posed by the rapid development of new communications and computer technologies.

The focus of the consultation was on the legal status of new electronic mail systems. The consultation was a natural followup to the first Project consultation held in June 1984 on the general issue of legal protection for private "data" or non-aural communications transmitted by wire and other electronic means.

Because of the considerable interest in the subject, we have prepared this conference summary for general distribution. We also include a summary of the conference discussion on possible privacy legislation in the 99th Congress and other ongoing privacy agendas.

The ACLU Privacy and Technology Project, headed by Jerry Berman, ACLU Legislative Counsel, is an effort to develop policy options to deal with privacy problems posed by new communications and computer technologies. A goal of the Project is to bring together privacy and technology experts, public interest and business groups, and key congressional staff to explore privacy/technology issues and policy options. The views expressed at the policy consultations do not represent a consensus or endorsement of any policy position by the participants. The Project is supported by grants from the Benton and Deer Creek Foundations. The Public Interest Computer Association, headed by Alan McDuffie, provides technical assistance and training to non-profit groups in the use of computers and assists the ACLU in conducting this series of privacy/technology consultations.

The January consultation on Electronic Mail was attended by experts on privacy law from several congressional committees; representatives from organizations such as the American Bar Association, Chamber of Commerce, and Washington Legal Foundation; technical experts from such corporations as GTE Telenet, AT&T, IBM, the Electronic Mail Association, and the Source Telecomputing Corporation; as well as independent experts such as Alan Westin of Columbia University, Robert Ellis Smith of the Privacy Journal, Ron Plesser, and John Shattuck, Vice President of Harvard University and former Director of the ACLU Washington Office. (See Appendix for List of Attendees)

## Privacy and the 99th Congress

Jerry Berman chaired the morning session which was devoted to a general discussion of privacy legislation confronting the new 99th Congress and other privacy efforts underway in 1985.

Ron Plesser of the Privacy Committee of the American Bar Association's Section on Individual Rights and Responsibilities outlined the Section's Privacy Project conducted in conjunction with George Trubow of the John Marshall School of Law in Chicago. After conferences in June and October of 1984, the ABA Project will spend 1985 exploring privacy/technology issues and developing recommendations for adoption by the American Bar Association House of Delegates to update current law. ABA conferees last year expressed considerable interest in ensuring the privacy of data communications and electronic mail. Plesser thought that a broad-based coalition could be developed around these issues. The long range goal of the ABA Project is to establish a government data protection entity to monitor federal government compliance with the Privacy Act of 1974.

Priscilla Regan of the congressional Office of Technology Assessment described its current assessment of "Federal Government Information Technology: Congressional Oversight and Civil Liberties." The study, expected to be completed in the fall of 1985, is exploring the privacy implications of technology management, computer security, data protection, government surveillance technology (via, e.g., computers, data interception, and video surveillance), and computer matching and profiling.

### Legislative Developments In the Last Congress

The conferees noted increased congressional interest in privacy legislation. Several privacy related bills passed in the 98th Congress.

**Cable Subscriber Information:** As Ron Plesser reported, Congress passed the Cable Telecommunications Act last year which requires a cable company to report to its subscribers what personal information about them is collected, used, and disseminated, and prohibits companies from releasing any "personally identifiable information" without notice and consent. The companies are required to specify what information may be disseminated unless a subscriber indicates an objection when he or she subscribes. A government entity may not obtain "personally identifiable information" about subscribers from a company without a court order, and the cable company must notify the subscriber of precisely what information is requested and give him or her fourteen days in which to object to the order in court. The government must show that the person is reasonably suspected of criminal activity and that the information sought is material evidence in a case to obtain a court order. This standard is the strictest privacy protection for record information ever enacted into federal law.

**Computer Matching:** Jerry Berman noted that in 1984 the Congress for the first time established some due process requirements to deal with the potential abuse of "computer matching." Computer matching is a process whereby separate files are run through a computer with a program set to detect predetermined "matches" of information in order to ferret out fraud and abuse in government programs. Although the Privacy Act of 1974 embodies the principle that personal information collected for one purpose may not be used for another unrelated purpose without notice and consent, computer matching programs often violate this principle. Nevertheless matching has been interpreted to meet the "routine use" exception to the Privacy Act's notice and consent requirements and has itself become routine. In 1984 the Budget Reconciliation Act authorized expanded use of IRS earned and unearned income records for matches involving federal and state social benefit programs. However, Senator William Cohen (R.MA) added amendments which prohibit the government from withholding benefits solely on the basis of a "match" which may indicate a recipient is not entitled to a benefit. The government must now (1) notify the subject that the information he or she provides is subject to matching; (2) independently verify the match to determine whether or not the recipient is entitled to a benefit; and (3) afford a person a due process hearing before benefits are denied or terminated.

**Computer Crime:** Last year Congress passed several sections of H.R. 5516, federal computer crime legislation sponsored by Rep. William Hughes of New Jersey. One section makes it a crime for any person to gain unauthorized access to bank or credit records. Another section makes it a crime for federal employees to disclose personal information protected by the Privacy Act without authorization. However, the section is so broadly worded that it covers non-sensitive government information and was opposed by several senators and representatives sympathetic to the privacy goals of the legislation. Efforts will be made this year to narrow the scope of this section to cover only records protected by the Privacy Act (S. 610, introduced by Sens. Charles Mathias, Patrick Leahy, and Edward Kennedy) and to expand computer crime provisions to protect other private data bases from unauthorized access (H.R. 1001, introduced by Rep. William Hughes).

## Privacy Legislation in the 99th Congress

The conferees then turned to the prospects for significant privacy legislation in the current Congress. Jerry Berman called on several hill staffers to discuss possible legislative initiatives in addition to the computer crime bills discussed above.

**National Crime Information Center:** Catherine LeRoy, Chief Counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights chaired by Rep. Don Edwards (D.CA), mentioned the possibility of legislation to require congressional authorization for the FBI to add intelligence and investigative files into the Bureau's National Crime Information Center (NCIC), a national computer system linked to over 60,000 police and criminal justice agencies. Over the last decade and a half, the principal function of NCIC has been to provide police access to relevant public record criminal justice information such as arrest records, wanted persons, stolen vehicles, etc. Recently, however, the FBI has been moving in the direction of adding intelligence and investigative files based on subjective investigative judgments for surveillance and tracking purposes (queries on the system help to locate suspects). In the late 1960's, the FBI added a "stop index" of anti-war and civil rights activists. When disclosed, the file was terminated because of congressional and public concerns about privacy. In 1983, however, the FBI, without legislative authorization or serious objection, added a "Secret Service" Index of persons belived to be dangerous to Secret Service protectees. Building on this precedent, the Bureau has under consideration files on suspected white collar criminals (Economic Crime Index), terrorists and their associates, organized crime figures and their associates, and other such files. The subjective, inherently inaccurate nature of the information and the possibility of wide dissemination of the information raise serious privacy and due process concerns. Rep. Edwards is planning hearings on these intelligence files and is considering legislation to require congressional authorization before such files may be added to the NCIC system.

Jerry Berman pointed out that a long-standing privacy issue has been the inaccuracy of arrest records indexed and disseminated by the NCIC system. As John Podesta of Senator Patrick Leahy's (D.VT) staff noted, there is a growing demand for these arrest records. The nuclear power industry wants these records to check employees for security purposes. Public officials are demanding arrest records for day care workers and teachers to deal with the "child abuse" issue. In this context, Rep. Charles Schumer (D.NY) is proposing significant legislation (H.R. 2129) to improve arrest record accuracy in the NCIC system. The legislation would provide states with funds to upgrade their criminal justice record systems and would require them to meet accuracy and completeness standards in order to participate in the NCIC system. Berman believes the legislation could have the support of law enforcement as well as privacy advocates provided that various interested parties agree not to resolve access issues in the same legislation. This has stymied arrest record reform efforts in the past.

**Protection for "Data" Communications:** As discussed at the first ACLU-PICA consultation. current law does not provide adequate protection for "data" communications carried by wire. Title III of the Safe Streets Act of 1968 requires a judicial warrant only for the "aural acquisition" of wire communications. The Foreign Intelligence Surveillance Act of 1978 makes it a crime for a government official to intercept data communications without a court order but does not spell out the court order requirements the government must meet and does not deal with private interception of data communications. John Podesta stated that Senator Patrick Leahy is working on legislation to protect the contents of "data" communications either as free standing legislation; as an amendment to computer crime legislation; or as part of legislation to protect the contents of electronic mail. David Beier of Rep. Robert Kastenmeier's staff stated that Congressman Kastenmeier has a similar amendment in his proposed bill to update electronic surveillance laws, including the establishment of warrant standards for video surveillance.

**Video Surveillance:** David Beier and Deborah Leavy of Rep. Kastenmeier's staff said the congressman would introduce a revised version of last year's legislation that would set judicial warrant requirements for video surveillance. In the recent case of U.S. v. Torres, 583 F. Supp. 86 (N.D. Ill. 1984), reversed and remanded, No. 84-1077 (7th Cir. Dec. 19, 1984), Judge Posner, writing for the Seventh Circuit, held a judicial warrant issued for video surveillance of a house used by a Puerto Rican terrorist group suspected of making bombs met the requirements of the Fourth Amendment. The Court, while holding that Title III of the Safe Streets Act did not authorize video surveillance, decided that the court ordered surveillance met the warrant requirements of the Fourth Amendment by meeting the statutory warrant requirements specified for electronic surveillance under Title III. While fashioning this "common law" warrant, the Court called on the Congress to deal with the complex and difficult issues posed by video surveillance. In this context, Rep. Kastenmeier has drafted legislation (H.R. 5243) that treats video surveillance as legally equivalent to wiretapping but establishes more stringent requirements: the subjects to be watched must be notified after the surveillance ends (even those inadvertently watched); there is a ten day limit on surveillance; the warrant must be specific about the application and the subject; the government must exhaust all other methods available; and finally, if the government exceeds its legal mandate, the court can suppress all evidence gathered from the surveillance.

**Data Protection Agency:** According to Bob Gellman, Counsel to the House Government Operations Subcommittee on Government Information, Justice, and Agriculture, Rep. Glen English will introduce H.R. 1721 to establish a Data Protection Board. However, he foresees no action on the bill in the current political climate. The Administration is hostile, the Congress unreceptive, and the public apathetic. Nevertheless, it is important to keep alive the idea of an executive oversight mechanism to monitor government compliance with federal privacy laws and regulations. As detailed in a recent Subcommittee Report, privacy oversight under the Reagan Administration is almost nonexistent.

## PRIVACY OF ELECTRONIC MAIL

### Introduction

The focus of the discussion was on the legal privacy protection for electronic mail. To set the stage, electronic mail and the electronic mail industry were described.

### Electronic Mail: What is It?

Electronic mail is a form of personal correspondence conveyed with computers over public and private phone networks. Communication usually carried by conventional mail or telephone coversations is typed into a private computer terminal and sent out from the computer through standard telephone lines. The message arrives at the electronic mail company's computer and is stored in the addressee's mailbox until the addressee---if also a subscriber---calls up this databank and retrieves his or her mail. However, a record copy may be kept for some period of time. If the addressee does not subscribe to the service, the electronic mail company converts the correspondence into hardcopy and deposits the communication in the first class or priority mail stream to the addressee's house or office. The correspondence is then delivered with the rest of the mail.

Electronic mail systems in fact are far more complex and diverse. As described by Philip Walker, General Counsel to GTE Telenet, there are two types of services, the non-computer based system (a service similar to "ZAP mail" by Federal Express), and the computer based categories ("private" electronic mail (EM) systems, which may be internal, intra-agency or intra-corporation (like Citibank's inter-office electronic mail system); and "public" EM systems, which are privately owned but open to public use, like Telemail from GTE Telenet). He also contrasted "computer mailbox" service, which is a two-way, terminal-to-terminal communication, with "hard-copy delivery", where the message originates in a computer terminal, is converted to letter form, and then sent via the United States Postal Service to the addressee.

## Electronic Mail: Growth of the Industry

As described by Mike Cavanaugh, Executive Director of the Electronic Mail Association, the electronic mail industry is a 100 million dollar a year industry that has the potential of becoming a multi-billion dollar a year industry by the 1990's. Tens of millions of messages are carried by it presently and hundreds of millions of messages will be carried by it in the 1990's. By the end of the year, there will be an estimated one million electronic "mailboxes" in the United States. Cavanaugh added that with the standardization and interconnection of various systems, the market will grow rapidly. In addition, virtually every industrialized country in the world has at least one electronic mail system and with the recently agreed upon international EM Communications Standard, the market for electronic mail systems should open up even further. Although some companies tout electronic mail as "the nation's new postal service", it presently tends to replace telephone calls more than it does conventional mail.

Although at present electronic mail is used primarily in business, it has a number of useful personal and household-oriented applications as well. Like the telephone in the 1880's, electronic mail is presently a "hard-sell", but is predicted to eventually become a household item. The industry strategy is to convince the consumer to replace mail and telephone communications with electronic mail messages and letters.

## Legal Discussion Overview:

As a new form of "data" communication conveyed with computers over public and private phone networks, electronic mail protection poses similar and even more complex legal issues than considered at the first ACLU-PICA consultation on "data" communications. On the one hand, we have to consider the protection of electonic mail "data" when it is being communicated. On the other, we must consider what privacy protection exists for the "hard copy" when it is being held or stored by electronic mail firms for later dissemination to the addressee. We must also consider the legal ramifications of non-common carrier networks and the responsibilities of electronic mail vendors with respect to "personally identifiable information" about subscribers.

To discuss electronic mail in its present federal law privacy context, some of the same but also new ground has to be traversed as at the first consultation. To guide the discussion, the conferees were presented with a legal focus paper which described each point in an electronic mail transaction: (1) When the electronic mail is in the terminal of the sender, prior to transmission; (2) When the electronic mail is in the "stream of communication" (e.g. in a telephone line or in a microwave transmission); (3) When electronic mail is in the mailbox of the addressee, and/or within the databank of the electronic mail company; and (4) When the electronic mail is transmitted to the addressee electronically or a hardcopy deposited in the U.S. Postal Service mailstream. At each stage, the paper compares electronic mail to its conventional counterparts and the legal protection afforded them.

### 1. The Terminal of the Sender

The protection of electronic mail correspondence at this stage depends on whether the acquiring party is the federal government or a private individual or group. The conferees agreed that information stored in a personal computer is protected by the Fourth Amendment against unauthorized government search and seizure.

Private acquisition of information stored in a personal computer is not protected by the Fourth Amendment and unauthorized access to a personal computer has not been sufficiently addressed by current theft or computer crime laws.

### 2. Communications in Stream

Though electronic mail originates from the keyboard of a computer terminal, it travels over the same lines as a telephone conversation. And since most long distance voice transmissions are converted to a digital signal, and transmitted by satellite and microwave, a telephone conversation and electronic mail are often in a similar encoded state when in the stream of communication.

The consensus of the first ACLU-PICA consultation applied to electronic mail "data" communications is that the contents of such communications are inadequately protected under current law. As the conferees agreed, legal protection for the contents of "data" communications is in doubt. The Supreme Court has not addressed the question. Title III of the Safe Streets Act only establishes a judicial warrant requirement for government interception of voice communications carried by wire and applies only to common carriers. Title III only penalizes private parties who intercept voice communications. The criminal penalties of the Foreign Intelligence Surveillance Act (FISA) make it a crime for government officials to intercept "data" communications but do not specify what form of court order (e.g. subpoena? search warrant?) is required and establish no penalty for unauthorized private interceptions. The other applicable statute, the Communications Act of 1934, has been held not to apply to communications in the telephone network and to communications carried by non-common carriers.

John Podesta stated that legislation to amend Title III to protect "data" as well as voice communications would provide legal protection for electronic mail at this stage. John Elliff of the Senate Intelligence Committee staff asked that, in the absence of cases of government interception of data without a judicial warrant or an unsatisfactory Supreme Court decision, why should the Congress amend the law.

Jerry Berman stated that the contents of these communications deserved protection, and there was no reason why the Congress should not act, particularly since the Justice Department has indicated these communications deserve protection and that the law could be updated or clarified. There is no reason for the EM industry or users of the system to tolerate uncertain privacy protection or to risk what the current Supreme Court might decide. Because complex technical issues may be involved, Congress is the appropriate body to develop coherent law. Judge Posner said as much in the Torres case dealing with video surveillance.

### 3. Electronic Mail Storage

Once the message arrives over the phone lines at the Electronic Mail Company, it is stored in electronic "mailboxes" in the database of the company. At this point, the privacy protection of personal electronic mail correspondence is virtually non-existent and new issues are raised that were not dealt with at the last consultation.

The best example of the legal situation is presented by the case involving Source Telecomputing Corporation. In 1983, as part of a criminal investigation, a United States Attorney obtained a grand jury subpoena for all records including electronic mail messages concerning certain customers of Source under criminal investigation. The Government argued that a search warrant was not required and that the subscribers had no privacy interest in the records which, the government argued, belonged to Source. The Government in opposition to a Motion to Quash the subpoena cited United States v. Miller, 425 U.S. 435 (1976), the Supreme Court decision holding that customers had no privacy interest in bank records conveyed to a third party or delivered by a third party to the government. Source only turned over billing and subscriber data and resisted the broader subpoena request. Eventually, the Government stopped pursuing the electronic mail records, but the law remains unsettled. Thus, at present, there are no laws that require the government to obtain a search warrant before obtaining electronic mail or which prohibit a company from voluntarily turning over electronic mail. If this were conventional mail, a search warrant would be required.

Mr. Stratt of Source noted that the problem is in part created by the fact that it is common practice for the Source and other EM companies to retain past information that subsribers have entered into their computer, and that subscribers usually do not know or realize this. If the companies retained less information, the system would be less vulnerable to such government requests, but then the companies would not be able to provide an important service, the retrieval of past data wiped out by the subscriber that, upon second thought, the subscriber finds he or she needs.

Ron Plesser asked if it is the case with most EM companies that the subscriber doesn't know that all his or her information is stored, and whether the subscriber usually appreciates this feature. EM company officials replied that most customers are more worried about losing their past files than they are about the issue of whether or not their files are eventually wiped out or erased.

Jerry Berman stated that keeping the files for a shorter period would not solve the problem since, at present, the company could agree to cooperate with the government and turn over records in the shorter time frame or to keep records of persons under investigation. Investigators might only be interested in new mail rather than old mail-- such as when they obtain a mail warrant for regular mail in United States postal channels. Agencies could ask for a copy of all messages in particular electronic mailboxes or all hardcopy conversions when the addressee is not also a subscriber. The government is sure to argue that hardcopy conversion by a mail company defeats any "reasonable expectation of privacy" and is no different than a company backup record.

At this point, some asked if the companies had developed guidelines similar to the ones developed by the phone companies on how to handle government requests for their records. Mr. Walker of GTE stated that because most EM companies have not yet had to deal with the issue of government access or even extensive commercial uses for subscriber information, there has been no push for an industry-initiated code dealing with the subject. Robert Gellman said that while such a code would be useful, legislation should be passed before the government begins routinely asking for this information.

If legal protection is going to be extended to electronic mail at this stage, the Congress will have to distinguish between different forms of electronic mail in terms of protection afforded. As several conferees pointed out, there are private messages in electronic mailboxes or coverted into hardcopy by the EM company as well as bulletin board-type information available to subscribers or even to the public at large. Then there are company records containing personal information, ranging from copies of electronic mail messages to subscriber information.

Jerry Berman suggested that this situation might be compared to that of the cable companies under the new Cable Franchise and Communications Policy Act of 1984. Disclosure to third parties of personal information about subscribers is allowed "only when necessary to conduct the service" and subscribers have grounds to object to certain disclosures. Since law enforcement officials are not involved in providing the service, government access is denied. If the government wants personal record information from a cable company, it must obtain a court order based on a showing that the subscriber is reasonably believed to be engaging in criminal conduct and that the information is material evidence in the case. The subject is given notice and an opportunity to contest the government's request in Court. Adopting a similar scheme for electronic mail, Congress would then deal with investigative agencies seeking mail without wanting to give notice to the customer. A search warrant requirement could cover this. As in the wiretap area, notice to the target at some point may be necessary if, as in the wiretap situation, the person has no way of knowing of the surveillance (e.g. the electronic mail is copied for the government or a backup copy provided while the message is sent on). Notice is not given for regular mail surveillance but customers do have notice when the mail fails to arrive or is delayed.

### 4. Transmission to the Addressee

If the electronic mail is called up by an addressee subscriber using his or her computer, it enters the communications stream once again. Protection for the mail will turn on protection for "data" communications as discussed earlier. If a hardcopy is placed in First Class mail for delivery to a non-subscriber, the conferees agreed a search warrant would be required as it is to open regular mail.

## Unauthorized Private Access and Computer Crime

Phil Walker and other industry officials stated that the most immediate threat to electronic mail messages is posed by the computer "hacker", whether a high school student doing it for fun, a disgruntled employee acting with malice, or a computer criminal (an embezzler) or industrial spy. Unauthorized access could occur at any point: at the terminal of the message sender, in the stream of communication, at the electronic mail company, or at the terminal of the addressee.

Jerry Berman pointed out that if Title III is amended to cover "data" communications, it would be a crime for a private party to intercept such communications as it is now a crime for private persons to conduct non-consensual wiretapping under the Safe Streets Act.

Others pointed out that 26 or more states have now passed computer crime bills. These statutes should protect against unauthorized access at the point of transmission and at the point of receipt of electronic mail messages.

The question is whether separate federal computer crime legislation is necessary to protect against unauthorized access from an electronic mail company. Would state statutes suffice? Phil Walker argued that federal law was necessary to deal with the interstate nature of computer hacking. He gave the following example: If a person in state A gains unauthorized access to an electronic mail company's files in state B, state B is in a difficult position to enforce its law because the perpetrator or hacker is in state A. State A, on the other hand, has very little incentive to go after the hacker since the "theft" occured in another state. A federal response is necessary.

Jerry Berman pointed out that computer crime legislation sponsored by Rep. Hughes (H.R. 5616) would have handled some of these cases but the relevant sections did not pass. When it was pointed out that the ACLU had opposed the legislation, Berman argued that the ACLU did not oppose the substance of the computer crime provisions that did not pass the Congress last year. However, he had serious doubts if they would solve the problem posed by Mr. Walker and others. The Hughes bill would criminalize unauthorized access to computer data bases for fraudulant purposes, but a $5,000 minimum damage requirement might render it an ineffective deterrent. However, if the jurisdictional amount were lowered, some would object to the breadth of federal criminal law jurisdiction. Federal jurisdiction could be based on "interstate" computer crime but still might be over and under inclusive.

One solution offered by John Podesta, David Beier and others would be a special electronic mail computer crime statute to be included in legislation to protect the privacy of electronic mail against both government intrusion and unauthorized private interception or access. Narrowly drawn, such a statute would not have to set a minimum damage requirement and could attempt to deal with intangible harms such as invasion of privacy.

**Conclusion**

The consultation ended with general agreement that a specific law should be drafted, introduced, and passed setting forth strict standards and procedures by which law enforcement agencies could obtain electronic mail communications and messages and electronic mail company records and subscriber information in order to protect EM users' right to privacy. In addition, conferees suggested that Congress adopt a strict law protecting companies against unauthorized private access to and use of electronic mail transmissions or electronic mail company records. Both criminal penalties and civil remedies were needed.

**Recent Developments**

Since the consultation, Senator Patrick Leahy and his staff have been drafting legislation to protect electronic mail in consultation with the staffs of Senator Charles Mathias and Rep. Robert Kastenmeier. Industry representatives and other interested parties, including the American Civil Liberties Union, have been involved in the process. Legislation is expected to be introduced in the near future.

Revised 7/85
04PV005

IEEE TECHNICAL ACTIVITIES BOARD/UNITED STATES ACTIVITIES BOARD
COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY

Lynn W. Ellis
Chairman
(203) 227-0345

Richard Gould
Vice Chairman
(202) 223-4449

Edith T. Carper
Executive Secretary
(202) 785-0017

PLEASE REPLY TO:
12 Beechwood Lane
Westport, CT [illegible] USA

May 24, 1985

Rep. Robert Kastenmeier, Chairman
Subcommittee on Courts, Civil Liberties,
& the Administration of Justice
2137 Rayburn House Office Building
Washington, D.C. 20515

Dear Rep. Kastenmeier:

It has come to our attention that you are considering submitting in the 99th Congress a bill similar in nature to H.R. 6343 "Electronic Surveillance Act of 1984" which you submitted in the 98th Congress.

The comments given below are being submitted to you on behalf of the Committee on Communications and Information Policy (CCIP) of the Institute of Electrical and Electronics Engineers (IEEE). The IEEE is the world's largest technical professional society with about 250,000 members worldwide, 215,000 of whom live and work in the United States.

Our Committee endorses H.R. 6343 in principle. We support measures which protect against unauthorized penetration and access to information in computer and communications systems.

However, we would like to recommend that any future bill also include an amendment to the term "wire communication" to protect users of non-common carrier facilities (for example, private communications networks and "local" area networks for computers) furnished for the transmission of interstate and foreign communications against unauthorized interception of their communications.

1. The Current Definition of the Term "Wire Communication" Does Not Fit Current Communication Practices

The current definition of the term "wire communication" is as follows:

> (1) "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person

> engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications. 18 U.S.C.A. Sec. 2510(1) (emphasis added).

When the current definition was drafted in 1968, only common carriers, such as AT&T and Western Union furnished or operated facilities for the transmission of interstate or foreign communications. Today, nearly twenty years later, the situation has changed considerably. There are more common carriers, for example, MCI, GTE Sprint, and Allnet. More importantly, non-common carriers are furnishing and operating facilities for the transmission of interstate or foreign communications, for example, the computer networks operated by such companies as Boeing Computer Services, Control Data, and Source Telecomputing.

If the definition of the term "wire communication" is not amended to include facilities furnished or operated by non-common carriers, the Federal Wiretap Law will not protect users of such facilities from the unauthorized interception of their communications.

2. Amend the Phrase "engaged as a common carrier" to Read "engaged as a common carrier or otherwise"

In order to include facilities furnished or operated by non-common carriers within the definition of the term "wire communication," Section 2510(1) should be amended as follows:

> (1) "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier or otherwise in providing or operating such facilities for the transmission of interstate or foreign communications. (Underscore indicates language to be added.)

Similarly, Section 2510(5)(a), describing "ordinary course of business" exceptions, should be amended as follows:

> (5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire or oral communication other than -
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of business; or (ii) ~~being used by a communications common carrier~~ any person engaged as a common carrier or otherwise in providing or operating facilities for the transmission of interstate or foreign communications in the ordinary course of its business, or by any investigative or law enforcement officer in the ordinary course of his duties;

(Strikeover indicates language to be deleted, underscore indicates language to be added.)

### 3. The Proposed Amendments Do Not Impair the Regulatory Jurisdiction of States Over Non-Common Carrier Facilities Furnished for the Transmission of Intrastate Communications

The regulatory jurisdiction of the States over non-common carrier facilities furnished or operated for intrastate communications will not be impaired by the proposed amendments; the States retain their jurisdiction over such facilities.

For the situations where it is difficult to separate facilities used for intrastate communications from facilities used for interstate communications, there will be a conflict as to which authority, State or Federal, has jurisdiction. This conflict, however, will not be unique to the facilities furnished or operated by non-common carriers; the same conflict has existed for many years for the facilities furnished or operated by common carriers. The same reasoning and principles used to resolve intrastate/interstate conflicts for the facilities furnished or operated by common carriers can be applied to non-common carriers. (For decisions resolving such conflicts, see: North Carolina Utilities Commission v. F.C.C., 522 F.2d 1036 (4th Cir. 1977) and 537 F.2d 787 (4th Cir. 1976); Use of Recording Devices, 86 FCC. 2d 313 (Docket No. 20840, 1981) and 11 FCC 1033 (Docket No. 6787, 1947).

The potential for the intrastate/interstate conflicts for facilities furnished or operated by non-common carriers should not be used as an argument against amending the term "wire communication" to protect users of interstate facilities furnished or operated by non-common carriers. If that argument were to be accepted, why does the Federal Wiretap Law protect users of interstate facilities furnished by common carriers?

If we can be of assistance in providing you with other information, please call on us.

Sincerely,

Lynn W. Ellis.

Lynn W. Ellis

LWE/hef

**U.S. Department of Justice**

Office of Intelligence Policy and Review

*Washington, D.C. 20530*

May 20, 1985

Honorable Robert W. Kastenmeier
Chairman, Subcommittee on Courts,
  Civil Liberties and the Administration
  of Justice
U.S. House of Representatives
Washington, D.C.  20515

Dear Representative Kastenmeier:

Since your letter of October 19, 1984, seeking our views regarding H.R. 6343 (98th Congress), the Electronic Surveillance Act of 1984, we have obtained the comments of the several Department of Justice components whose activities would be affected by this bill and representatives of this office, the Justice Department's Criminal Division and the Office of Legislative and Intergovernmental Affairs have met with members of the Subcommittee staff to discuss its contents. We recognize that the bill was merely an initial effort to stimulate discussion of potential issues that were identified during the Subcommittee hearings that preceded its introduction. In order to assist you and the Subcommittee staff in assessing the advisability of the proposals in the bill, we are providing this preliminary analysis of its provisions.

Generally speaking, we agree that the Omnibus Crime Control and Safe Streets Act of 1968 [Title III] should be reassessed continually as experience and new technology are developed. In this regard, it should be noted that the President's Commission on Organized Crime is reviewing Title III and may recommend amendments to the statute. The Department of Justice will certainly propose amendments to the statute in the event that our continuing assessment of the law governing electronic surveillance reveals a need for such action in the future. Since we do not believe there are serious flaws in Title III or its implementation currently, however, we believe the statutory structure should not be modified at this time.

With regard to the Foreign Intelligence Surveillance Act of 1978 (FISA), we believe the record of judicial and congressional review demonstrates that the delicate balancing of interests embodied in FISA represents a fair and effective framework for the authorization and conduct of electronic surveillance in foreign intelligence investigations. Accordingly, we concur in the conclusions of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence that any proposals to amend FISA at this time are ill advised. H. Rep. No. 98-738, 98th Cong., 2d Sess. 10 (1984); S. Rep. No. 98-660, 98th Cong., 2d Sess. 24 (1984).

Furthermore, in considering any amendments in this area, the complex interaction between Title III and FISA must be carefully examined to avoid unforeseen consequences. Slight differences between Title III and FISA may have the effect of obstructing use of certain investigative techniques in foreign intelligence and counterintelligence investigations.

An example of the potentially adverse, but incidental, effects of amendments relates to the bill's proposal in sections 7 and 8 to require adherence to Title III for the use of "tracers" and "video surveillance" in circumstances in which the target possesses no reasonable expectation of privacy. This change would result in great difficulties in foreign intelligence investigations because of the fact that use of these investigative techniques under such circumstances may not constitute "electronic surveillance" under FISA. The inapplicability of FISA stems from the fact that the element of the definition of "electronic surveillance" that is intended to govern use of tracers and video surveillance is not met unless such technique is employed "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. §1801(f)(4). Thus, the FISA Court may possess no jurisdiction to authorize the activity, and yet it would constitute a criminal act under Title III if conducted without a court order. Since foreign intelligence investigations generally do not meet the criteria for a Title III order, it follows that there might be no lawful way to engage in the activity in most foreign intelligence cases. These untoward consequences evidence the need to exercise extreme caution in crafting amendments to these complex statutes.

In addition to these general observations, specific comments concerning each of the provisions of H.R. 6343 are set forth below.

## Section 2

Subsection 2(a) of H.R. 6343 would strike "aural" from the definition of "intercept," 18 U.S.C. §2510(4), thereby bringing within Title III's controls a variety of communications not currently governed by the statute. This would include, for example, telex communications, transmissions between computers, and radio communications to digital display pagers. The effect of this change would be two-fold; it would require the government to obtain an order under Title III in order to acquire such communications in the course of criminal investigations, and it would criminalize the interception of such communications if conducted outside Title III's framework, by private parties such as "computer hackers" for example.

One undesirable effect of this provision would be to draw the use of "pen registers" and "beepers" under Title III. The basis upon which we oppose applying Title III to these investigative devices is discussed below (Sec. 7). As for criminalizing "computer hacking," the same result, if intended, may be achieved by a more narrowly drawn provision that would not so adversely affect lawful law enforcement activities.

Subsection 2(b) of H.R. 6343 would expand Title III's definition of "aggrieved person," 18 U.S.C. § 2510(11), to include any person whom the "applicant" had reasonable cause to believe was involved in the activity being investigated. The effect of this change would be to extend standing to such persons for the purpose of filing suppression motions. 18 U.S.C. §2518(10).

This change would appear to create unnecessary obstacles to successful prosecutions by fostering substantial new opportunities for evidentiary hearings and inquiries into the state of knowledge and subjective intentions of law enforcement officers engaged in Title III activities. The Fourth Amendment is satisfied by the current definition of "aggrieved person" (parties to intercepted communications and persons against whom interceptions are directed). Alderman v. United States, 394 U.S. 165 (1969). Unless there have been significant injustices of which the Department is unaware, this change does not appear to be warranted.

Sections 3 and 6(e)

Section 3 of H.R. 6343 would amend 18 U.S.C. §2515 so as to authorize trial courts to suppress the contents of communications intercepted during a course of conduct demonstrating a pattern of intentional violation of the minimization requirements of 18 U.S.C. §2518(5). Subsection 6(e) of the bill would amend 18 U.S.C. §2518(5) to require that every order under Title III include the provision that interceptions be conducted "with the good faith intent to minimize." Thus, the combined effect of these provisions would be to authorize suppression of the contents of communications intercepted during a course of conduct demonstrating a pattern of "bad faith" noncompliance with minimization requirements.

While the substance of these provisions is laudatory since all interceptions are being, and should continue to be, conducted in "good faith" compliance with minimization requirements, these provisions as drafted would make the subjective intent of the investigative agents relevant to the lawfulness of surveillances and subject to evidentiary hearings. While such hearings would ultimately demonstrate that the surveillances have been conducted in "good faith" compliance with minimization requirements, they would undoubtedly protract and complicate prosecutions while providing little, if any, tangible benefit to the public. An objective standard of "reasonableness" with regard to compliance with minimization requirements would more closely capture the approach taken by courts in exercising their discretion to suppress the contents of communications as necessary to serve the interests of justice. Again, barring evidence of significant injustice under this current practice, amendments in this area may serve only to hinder the judicial process.

## Section 4

Section 4 of H.R. 6343, which would add sections 1512 and 1513 of Title 18 to those offenses that may underly Title III applications, 18 U.S.C. §2516(1)(c), has been rendered moot by enactment of § 1203(c)(2) of the Comprehensive Crime Control Act of 1984, P.L. 98-473.

In this regard, however, further amendment of 18 U.S.C. §2516(1)(c) to include as an underlying offense 18 U.S.C. §2312, which prohibits interstate and foreign transportation of stolen motor vehicles and aircraft, may be appropriate. This change would have the potential for facilitating investigations into the growing problem of organized auto theft rings and so-called "chop shop" operations.

## Section 5

Section 5 of H.R. 6343 would amend 18 U.S.C. §2517(5) which authorizes law enforcement officers to use and disclose, in the performance of their official duties, the contents of intercepted communications that "relate" to offenses other than those specified in the authorization order. The current provision also authorizes such contents to be used in evidence upon judicial approval that such contents were intercepted in accordance with Title III.

By inserting the word "solely" after the word "relate," this proposal would authorize use of the contents of communications that "relate solely" to offenses other than those specified in the order of authorization. It is unclear, however, as to what effect this change would have on the use of contents of communications that merely "relate," but do not "relate solely," to other offenses. Whether the intent is to prohibit or permit use and disclosure of such contents in various circumstances is uncertain. This provision requires clarification.

Section 6

Subsection 6(a) of H.R. 6343 would amend 18 U.S.C. §2518(1)(b) to require that every application for a Title III order include "the specific investigative objectives and the specific targets" of the interception. Including "the specific investigative objectives" of the surveillance in each application reflects current practice. Requiring that every application include "the specific targets" as well would cause serious problems when considered together with the change proposed in subsection 6(d) of the bill.

Subsection 6(d) would amend 18 U.S.C. §2518(4) to, among other things, prohibit interception of any communication pursuant to a Title III order

> unless at least one of the parties to such communication is identified in such order, the court issuing such order found probable cause that virtually everyone using the designated facility or telephone is doing so for the purpose which is the object of investigation set forth in the order, or for the purpose of monitoring to become familiar with the voices of targets set forth in such order.

The requirements of subsections 6(a) and (d) would effectively prohibit the government from intercepting conversations of unidentified conspirators in many instances.

Current practice is to seek Title III orders that permit interception of the conversations of identified targets as well as "others as yet unknown." Such persons are then added to the list of identified targets as they become known and probable cause is acquired to obtain their communications. This enables the Department to develop prosecutions against individuals who are unknown upon initiation of electronic surveillance but who are determined to be members, and sometimes leaders, of criminal conspiracies during the course of a surveillance. Since unknown individuals cannot be identified as "specific targets" of surveillance for purposes of inclusion in initial applications, the effect of subsection 6(d) would be to prohibit interception of their conversations unless one of its three limitations is met. As a practical matter, these limitations could not be met in many instances and the government would be forced to forego interception of a substantial volume of conversations evidencing criminal activities to the detriment of further investigations and prosecutions.

Subsection 6(b)(1) would amend 18 U.S.C. §2518(1)(c) to require that the statement in Title III applications regarding less intrusive means specify certain investigative techniques as having been tried and failed, or as reasonably appearing unlikely to succeed if tried or too dangerous. This provision is consistent with current practice.

Subsection 6(b)(2) would likewise amend 18 U.S.C. §2518(1)(c), to require that the statement regarding less intrusive means "establish" that use of such techniques would reasonably appear unlikely to succeed or be too dangerous. There are two difficulties with this change. First, it is simply not feasible in many circumstances to forecast, beyond mere speculation, the effect or likely success that will follow from an effort to use certain techniques in a particular investigation. While a particularly well placed, reliable and intelligent informant may provide as much or more information as an electronic surveillance, such ideal assets are difficult to find and may require months of assessment and development before their true value can be adequately evaluated. Second, the standard that would be created implies some degree of proof that could not be met in many cases. The government cannot do more in this area than explain in an objective fashion the considerations that appear to make other means impractical. To require some form of positive proof of this conclusion, as is inferred by use of the term "establish," may be read to compel the government to conduct ancillary investigations into the availability of various investigative techniques.

Subsection 6(c) of the bill would amend 18 U.S.C. §2518(3) to empower a court to authorize interception of communications outside its territorial jurisdiction in the case of a mobile interception device installed within such jurisdiction. While we believe this provision should be modified to make clear that it is not intended to empower courts to authorize surveillances outside the territorial jurisdiction of the United States, it would be a useful response to the problems that are caused by the increasing use of mobility by criminal elements to thwart government investigative efforts.

Subsection 6(d), in addition to the provision discussed earlier in conjunction with subsection 6(a), provides that use or disclosure of communications intercepted by an automatic recording device shall be treated in the same manner as communications intercepted without such a device. The intent of this provision is uncertain and warrants clarification.

Subsection 6(d) would also authorize courts to grant orders authorizing physical entry to install interception devices, but only upon a showing "that there are no less intrusive means of effecting the interception." Under the reasoning of Dalia v. United States, 441 U.S. 238 (1979), no additional statutory provision is required for courts to grant such authority. If any amendment of this nature is necessary, however, it should be modeled upon the analogous provision of FISA [50 U.S.C. §1805(b)(1)(D)] and empower courts to authorize government agents to engage in physical entries in the course of conducting electronic surveillance when the courts deem appropriate. The provision should not require the government to show that absolutely no less intrusive means of effecting the interception are available. At minimum, a "reasonableness" standard should be used instead so that factors beyond theoretical availability, such as the danger, cost and exotic nature of alternative means, may be considered.

Subsection 6(f) of the bill would amend 18 U.S.C. §2518 to require that the judge issuing the order receive, not less than "fortnightly," reports showing what progress has been made toward achievement of the objective of the surveillance, the need, if any, for continued interception, and whether any evidence of offenses other than those specified in the order has been discovered. This provision would also authorize the judge to suspend or terminate interception if any report is deficient, evinces serious procedural irregularities, or indicates the legal basis for interception no longer exists. This provision might tend to lengthen and standardize at 14 days the period between reports since the period now varies and many judges now allow only seven or 10 day intervals.

Subsection 6(g)(1) would amend 18 U.S.C. §2518(7) to allow for the interception of communications without a court order upon determination of the existence of an emergency situation with respect to "conspiratorial activities of a life-threatening nature." This proposal appears to be subsumed and rendered moot by §1203(b) of the Comprehensive Crime Control Act of 1984, P.L. 98-473, which amended Title III to authorize "emergency surveillances" in situations involving "immediate danger of death or serious physical injury to any person."

Subsection 6(g)(3) would amend 18 U.S.C. §2518(7) to require that oral notice be provided to a judge of competent jurisdiction prior to initiation of an "emergency surveillance." This provision may be unworkable because it is simply infeasible to require contacting a judge in these circumstances, especially in sparsely populated judicial districts served by few judges. A similar provision now appears in FISA [50 U.S.C. 1805(e)] but is practical there only because the FISA Court is very small and localized. Thus, there is always at least one judge available in the Washington, D.C. area. Given that the authority to conduct "emergency surveillances" contemplates life-threatening situations, it seems imprudent to risk tying the government's hands in such circumstances. Concerns for prudence and accountability in using this emergency power are adequately addressed by retention of the current requirement that an application for an order approving an "emergency surveillance" be made within 48 hours after the interception has occurred or begins to occur. 18 U.S.C. §2518(7).

Subsection 6(h) would amend 18 U.S.C. §2518(8)(a) to permit submission of recordings of intercepted communications to the judge issuing the order within "48 hours after" expiration of the period of the order (or extensions). The current provision requires such a submission "immediately upon" expiration of the period of the order (or extensions). This change would be helpful in clearly stating a reasonable period for compliance.

## Section 7

Section 7 of H.R. 6343 would add a new section to bring the use of "pen registers" and "tracers" under Title III. This change would seriously encumber the law enforcement program that has developed under Title III.

Pen registers, as defined in the bill, are devices that attach to telephone lines for the purpose of identifying and recording dialed numbers. Their use invades no constitutionally protected interest. Smith v. Maryland, 442 U.S. 735 (1979). Thus, whether to include them within Title III turns upon the balance between their utility in law enforcement investigations and the infringement of the privacy interests of persons against whom they are targeted.

For years pen registers have been a valuable technique in criminal law enforcement investigations. This is especially so in investigations into criminal activities such as drug trafficking and bank fraud that are frequently perpetrated through electronic communications. Under current Department practice, court orders authorizing use of pen registers are obtained under Fed. R. Crim. Proc. 57(b) by Assistant United States Attorneys in the field without the review and approval of senior Department officials. Inasmuch as Rule 57(b) does not require a showing of "probable cause" to obtain such an order, pen registers have proved especially useful in the earlier stages of investigations when the primary objectives are identifying participants and determining generally their relationships in the alleged criminal activity. In many instances, in fact, the results of pen registers are then used to develop the more detailed showing of "probable cause" necessary to obtain Title III orders authorizing the interception of communications.

The effect of subjecting the use of pen registers to Title III's controls would be to limit their use to those investigations in which "probable cause" has been previously developed through the use of other investigative techniques, and to impose upon their use Title III's elaborate procedure of review and approval by senior Department officials prior to submission of applications to court. As a result, it is virtually certain that pen registers would be used much less frequently than is now the case, to the detriment of criminal investigations and ultimately prosecutions. Given that pen registers, by comparison to interception of communications, constitute a minimal intrusion into the privacy interests of targeted subjects, it seems unnecessary and inappropriate to bring their use within the controls of Title III.

The inclusion of "tracers," or "beepers," under Title III would similarly impact adversely on law enforcement efforts. In most instances the use of tracers, like pen registers, invades no constitutionally protected interests. E.g., United States v. Knotts, 103 S.Ct. 1081 (1983). In these instances, court orders authorizing their installation and monitoring are obtained, as with pen registers, under Fed. R. Crim. Proc. 57(b) by Assistant United States Attorneys in the field without the review and approval of senior Department officials. In those cases in which the installation or monitoring of tracers would invade a subject's reasonable expectation of privacy, e.g., United States v. Karo, 104 S.Ct. 3296 (1984), court orders, pursuant to a showing of "probable cause," are sought under Fed. R. Crim. Proc. 41. In these instances as well, however, review and approval of applications by senior Department officials is not required.

Like pen registers, tracers are an effective investigative tool, especially in drug investigations where they are used to track shipments of contraband and vehicles that transport those shipments. Their use often eliminates the need to devote the enormous number of resources that are required for a "moving" physical surveillance. The practical effect of subjecting the use of tracers to Title III's controls would be to narrow severely the circumstances in which they could be effectively employed. Inasmuch as tracers, like pen registers, very rarely involve any infringement into the privacy interests of the target, it seems imprudent to impose upon their use the strict requirements and panoply of procedures and controls mandated by Title III.

## Section 8

Section 8 of the bill would add a new §3117 to Title 18 U.S.C. and thereby bring within Title III "video surveillance," a term defined in the bill to mean "the recording of visual images of individuals by television, film, videotape, or other similar method, in a location not open to the general public and without the consent of that individual." This formulation of "video surveillance" would appear to regulate a much broader scope of government activities than is appropriate.

The government would be required to proceed under Title III whenever the target is in any area "not open to the general public." While the phrase "not open to the general public" is subject to more than one interpretation, a fair reading would require a Title III order whenever the location of the target is not open to free and ready access by any member of the public. Such an interpretation of this provision would include a variety of locations, such as residential yards and front porches, that are readily observable from public areas and emdody no reasonable expectation of privacy for Fourth Amendment purposes. Requiring the government to obtain a Title III order to surveil an individual at such locations would severely limit potential use of the technique, making important evidence either unavailable or available only through use of less efficient investigative techniques (e.g., 24 hour physical surveillance). This result illustrates that this provision strikes an inappropriate balance between effective law enforcement and protection of civil liberties.

The definition of "video surveillance" further suffers from an unreasonably narrow "consent" exception. This provision would have the effect of excluding from Title III only surveillances conducted with the consent of the targeted individual. Inasmuch as the law that has developed under the Fourth Amendment recognizes that any individual who is present at the targeted location may "consent," this definition would seem to restrict unnecessarily the government's ability to employ this technique.

## Section 9

Subsection 9(a) of H.R. 6343 would allow suppression of evidence obtained or derived from a FISA surveillance if the primary purpose for acquiring that portion of such surveillance was to obtain information to be used in a criminal proceeding. We recommend that this provision not be enacted for the following reasons.

FISA, as presently enacted, requires that each application contain a formal certification by a senior official of the executive branch that the purpose of the surveillance is to acquire foreign intelligence information, that designates the type of foreign intelligence information being sought according to category, and that includes a statement specifying the basis for the assertion that the information sought is the type of foreign intelligence described in the application. 50 U.S.C. §1804(a)(7).

This legislative proposal would require instead that every "portion" of a FISA surveillance satisfy in hindsight the "primary purpose" test. The effect of its enactment would be detrimental to prosecutions derived in part from FISA surveillances, where information concerning criminal activities is acquired only incidentally. For example, if during a FISA surveillance of a terrorist group the government learns that the group is financing its terrorist activities through narcotics trafficking, public policy should permit the use of such information in subsequent prosecutions. The dilemma presented by subsection 9(a) is that each piece of evidence would have to be examined by a court solely in light of whether the "primary purpose" of the surveillance at that point in time was the incidental narcotics-related interceptions.

Viewed from another perspective, this proposal would appear to penalize the government for anticipating that the fruits of a FISA surveillance may eventually be used as evidence in a criminal trial. By requiring the courts to consider the primary purpose of every portion of a FISA surveillance rather than the primary purpose of the surveillance in its entirety, the proposed section seeks to impose rigid distinctions between foreign intelligence and law enforcement purposes that do not take into account the reality of counter-espionage and counter-terrorism investigations. For example, the primary objective of a counter-terrorism investigation is obviously to stop terrorists from committing acts of violence. Identification of the network of terrorist agents is only a first step toward that objective. The ultimate goal in almost every investigation is to deal with the activities of the terrorists whether it be by their apprehension and prosecution here or abroad, by deportation from this country, by interdiction of weapons shipments, or by other lawful measures. Such methods of dealing with a single terrorist cell occur within the context of the FBI's investigation of the overall international terrorist organization. It provides little solace to have identified a cell of international terrorists bent on assassinating foreign officials or diplomats in the United States, or bombing diplomatic establishments, if no further action can be taken other than to identify members of the group.

The proposed section also creates a presumption of inadmissibility as to all evidence obtained from a FISA surveillance not more than 30 days before the return of an indictment. This legislated presumption of illegality, however, is in direct conflict with the presumption of validity which the Supreme Court has attached to the warrant process. In Franks v. Delaware, 438 U.S. 154, 171(1978), the Court noted that the warrant process brings with it a "presumption of validity with respect to the [application] supporting the ... warrant." The proposed legislation would negate this presumption, nullify the certification as to the purpose of the surveillance, as well as require that the government meet the burden of proving not only that the overall purpose of the surveillance was to collect foreign intelligence information, but also that every interception had this as its primary purpose -- facts which may be difficult to prove in situations where, as already noted, there exists a coalescence of foreign intelligence and law enforcement objectives.

Further, the proposed presumption obviously may result in courts ruling certain surveillances illegal because the government could not overcome the burden of proof as to a certain portion of the surveillance. Such rulings may result in constitutional tort actions being filed against government officials. It is unclear whether this presumption is intended to apply also to weaken the good faith immunity defenses that are available in such civil actions.

In summary, by creating this presumption of inadmissibility, the proposed section would in effect repeal section 106 of FISA, which, in allowing the use of FISA-derived information in criminal proceedings, has been upheld by the highest federal court to have considered the issue. United States v. Megahey, 743 F.2d 59 (2d Cir. 1984). The ultimate effects of the proposed section would likely be an adverse impact on the options available to the U.S. government to meet espionage and terrorist threats from abroad and a windfall to hostile foreign intelligence and international terrorist organizations that may be contemplating the conduct of operations in this country.

Subsection 9(b) of the bill would require the congressional intelligence committees to report on an annual basis respectively to the House of Representatives and the Senate concerning the implementation of FISA. This provision is properly a matter within the province of the legislative branch.

Subsection 9(c) of the bill would require that the executive branch disclose the approximate number of individuals, within a range of 10, who have been the targets of FISA surveillance. This information would permit hostile foreign intelligence services to compile information concerning the extent to which the government is aware of the activities of foreign agents. Sophisticated intelligence services of hostile governments, as a result, might well be able to estimate the number of their own establishments and intelligence officers and agents under electronic surveillance. Such disclosures may serve to encourage hostile foreign intelligence operations in this country. On the other hand, it is unclear what public interest or purpose would be furthered by the publication of such figures.

Subsection 9(d) of the proposal would require that the government notify United States persons whose communications have been intercepted in FISA surveillances of the fact of such interception not later than 180 days after the end of surveillance, unless the government can show "by clear and convincing evidence" that such disclosure would jeopardize an ongoing intelligence operation or intelligence sources or methods. This proposal would create an unreasonable burden, particularly with respect to surveillance directed at foreign powers. Many of these surveillances are continuous, making impractical the notification of all United States persons who are overheard. This problem is exacerbated by the difficulty in determining in particular cases whether a communicant is a United States person.

Assuming that a party to a conversation can be identified as, or presumed to be, a United States person, the duty to notify would turn on the intelligence significance of that person's communications. Since the intelligence significance of individual communications might not be readily ascertainable, the government in many instances would not be able to establish "by clear and convincing evidence" that disclosure would jeopardize our national security interests. In such instances, we may find, after notification and based upon subsequently collected intelligence, that such notification had proved detrimental to these interests.

Lastly, the proposed notice requirement appears predicated on the assumption that FISA electronic surveillances and investigations are terminated at the same time. This is not always the case inasmuch as a surveillance may also be terminated because it is not productive, resource limitations and altered priorities require shifting to other targets, or for technical considerations.

The Office of Management and Budget has advised that there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,

for Mary C. Lawton
Counsel for Intelligence Policy

# STATEMENT OF UNIDEN CORPORATION OF AMERICA ON H.R. 3378, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986.

Before the House Subcommittee on
Courts, Civil Liberties, and the
Administration of Justice.

Uniden Corporation of America ("Uniden") herewith submits its comments regarding H.R. 3378, proposed legislation to amend the provision of Title III of the Omnibus Crime Control and Safe Street Act of 1968 ("Omnibus Act") relating to the interception of private communications through wiretapping and eavesdropping. 18 U.S.C. § 2510 *et. seq*. H.R. 3378 would extend the protection accorded such communications to encompass, with certain exceptions, messages transmitted via "a wire, radio electromagnetic, or photoelectric system that affects interstate or foreign commerce."

## I. INTRODUCTION

Among its business interests, Uniden manufactures a variety of radio transmitting and receiving equipment, including scanners bearing the trademark "Bearcat." Scanners are simply receivers which have the technology to rapidly review in succession many frequencies of the radio spectrum seeking a channel that is energized with radio frequencies. The user may thereby rapidly identify a channel that is in use. Scanners have proven to be popular products with the public and socially beneficial. Millions of hobbyists and radio enthusiasts have purchased scanners to make radio more useful and enjoyable to them. In some cases, lives have been saved by their use, such as when they have been used to head off a terrorist plot against Israel. However, because of the detrimental effect H.R. 3378 will have on manufacturers, retailers, and users of these radio receivers, Uniden respectfully submits and appreciates the opportunity to present its comments for the published record.

Uniden certainly supports the concept of H.R. 3378 and agrees with Representatives Kastenmeier and Moorhead and their Senate colleagues, Senators Mathias and Leahy, that the existing wiretap and eavesdropping laws have not kept pace with the recent developments in digital data and telecommunications technology, and thus need revision in order to adequately protect the new technology.

Uniden's primary concern, however, is that the bill, in its present form, is vague, overly inclusive, and may have far-reaching, yet unintended, effects on the public. First, H.R. 3378, in its present form, encroaches upon valued First Amendment freedoms which have been protected by the judiciary and the legislature throughout the history of our democratic government. Second, the bill has significant international implications which are inconsistent with stated United States positions on the free-flow of data in the international arena. Third, because the bill does not establish a reasoned standard upon which to protect telecommunications, enforcement by the state and interpretation by the judiciary will entail onerous, perhaps impossible, burdens.

## II. DISCUSSION

### A. First Amendment Freedoms

Section 101(g) is so vague in its present form that it may inadvertently infringe upon the safeguarded freedoms of the American public which are encompassed by the First Amendment. For example, the Supreme Court has observed that the First Amendment involves not only rights which protect free speech, but also rights for the public to hear and listen to various voices in society. See Red Lion Broadcasting Co., Inc. v. FCC, 395 U.S. 367 (1969). The First Amendment guarantees to the listener the right to obtain information by a variety of means and from a variety of sources. Without such guarantees, the speaker's right of expression is meaningless. Moreover, a fundamental tenet of our form of government is the belief that "the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public." Associated Press v. United States, 326 U.S. 1, 20 (1945).

H.R. 3378 establishes a dangerous precedent for denying the general public open access to the free flow of information across domestic and international borders. While the legislation is not necessarily intended to interfere with valued social freedoms, the language of the bill is so vague and broad that it could create a basis for regulatory abuses in other areas. For example, the U.S. government has demonstrated its commitment to the free flow of information on a global scale before the United Nations and through participation in international agreements. In addition, Radio Free Europe and the Voice of America are two institutions committed to this ideal. As some societies which attach little significance to personal freedoms have demonstrated, one method of subverting the free exchange of ideas is to enact laws which prohibit people from tuning in to certain bands of the radio spectrum. While H.R. 3378 was clearly not intended to be used in this manner, imposing the kind of prohibition proposed by Section 101(g) is alien to the manner in which our society typically approaches matters relating to the free flow of information and ideas.

In areas involving such fundamental rights, courts have traditionally searched for the narrowest, least intrusive means of accommodating two conflicting values. This is particularly true if government regulation would somehow affect a highly valued freedom, such as freedom of speech. Uniden submits the bill as presently written has not observed such an approach.

Admittedly, the Supreme Court has also stated that the Fourth Amendment prohibition against unreasonable searches and seizures by the government includes a reasonable expectation of privacy with regard to the use of a land line telephone. Katz v. United States, 389 U.S. 347 (1967). Although concern for individual privacy against intrusions by other persons is important, the Court's concern in Katz focused primarily on improper government intrusion into the private affairs of individual citizens. Individual privacy not involving the government has largely been accommodated through providing individual rights of action in the courts for the offended party.

By contrast, H.R. 3378 gives the federal government an affirmative right to prosecute citizens for even inadvertently intruding upon the privacy of other citizens. Uniden submits that this is a highly inappropriate function for government. Traditionally, it has been the responsibility of each individual citizen to ensure his or her own privacy vis a vis other private citizens. The function of government in this case should be to give individuals the tools needed to secure their privacy. Uniden believes that a similar approach should be followed in the crafting of this legislation.

B. H.R. 3378 is Overbroad

In addition to the First Amendment problems discussed above, the proposed statute also criminalizes innocent use of scanners. By its terms, the bill seeks to ensure privacy to cellular telephone users. These telephones operate on frequencies in the 806 to 912 MHz band. While it is true that some scanners can receive signals on these frequencies, many other receivers which have been on the market for years can do so as well. For example, conceivably their existence would moot the purpose of Section 101(g) since it is intended only to apply to frequencies not generally available to the public. In addition, television sets which were manufactured beginning in the 1960's, and are still widely used today, can also receive transmissions in this band of the radio spectrum on their UHF tuners.

However, neither the scanners nor the televisions were designed to intercept, track or tune into conversations conducted on cellular telephones. There are two key factors that render the chances of intentionally intercepting a particular conversation on a cellular telephone remote. First, scanners and cellular telephones employ different channel spacings. Specifically, most scanners employ 12.5 MHz channel spacings while cellular telephones utilize 30 KHz spacings. Second, cellular telephone systems are designed so that operating frequencies are constantly changed as a mobile unit traverses from one cell to another. Due to the different channel spacings and the constant change of frequencies, it is virtually impossible to intentionally intercept a specific conversation on a cellular telephone with a typical scanner device. Nevertheless, the language of H.R. 3378 makes even the random momentary interception of a cellular phone call unlawful, notwithstanding the FCC rule that a cellular telephone operation must scan all cellular frequencies to determine which channels are unused before setting up a circuit for a new telephone call. Thus, unlike most criminal statutes, culpability under H.R. 3378 would not depend on intent. Even an inadvertent interception, by someone who did not even realize what he or she was hearing, would violate the proposed law and a strict construction could create a violation by every cellular user.

C. Enforcement

Given the broad scope of H.R. 3378, innocent short wave, scanner and household television operators could be guilty of criminal violations. The broad sweep of the bill also raises critical issues with respect to enforcement. It will be impossible for the police to carry out any truly meaningful enforcement effort. Legislating privacy in this fashion not only creates a false sense of security contrary to the public interest, but also cannot accomplish the valid social objectives the Congress wishes to advance. With H.R. 3378 in its present form, cellular telephone users will rely on the police power of the state to ensure that their conversations are not overheard. While this concept may be appealing in theory, the practical application is problematic at best.

First, according to Representative Kastenmeier, the bill is not intended to outlaw the manufacture, retail or use of receiver equipment. Thus, unlike burglary tools, possession of receivers is not (and could not be) an offense. Second, there are no physical indications which provide tangible evidence of the interception of cellular conversations. Unlike a wiretap that produces a physical trespass on copper wire, the only possible evidence of an interception of a cellular transmission would be eye witness testimony or a tape recording of the conversation. Assuming there is no eye witness to the illegal interception, an individual would never know that his or her cellular phone conversation was intercepted, except through possible subsequent use or disclosure of the information discussed.

For this reason, both case law and legislation which have dealt with the interception of private communications have focused on the _use_ of intercepted messages. For example, as in _Katz v. United States_, discussed above, where private messages were illegally intercepted by the government, the typical circumstance involves the government using wiretaps to gather evidence for criminal prosecutions. The remedy developed by the courts to curb such abuses is the exclusionary rule which bars all use of evidence collected as the result of improper eavesdropping. Similarly, Section 705(a) of the Communications Act of 1934, as amended, ("1934 Act") prohibits the divulgence of information intercepted over radio except through properly authorized channels. In other words, under the 1934 Act it is a federal crime for private citizens to divulge information obtained as the result of overhearing a private radio transmission.

There are two main reasons that Katz and Section 705(a) have focused on the use or divulgence, rather than the mere interception, of private messages. First, without such use, no demonstrable harm has been committed. Second, unless someone actually acts on private information obtained as the result of the eavesdropping, the fact that such an invasion of privacy occurred may never be known. Under such circumstances, any attempt to legally prove an invasion of privacy has occurred would be impossible. Consequently, because of the lack of harm and the difficulty of proof, both case law and legislation have focused on use or divulgence rather than interception. Congress should follow a similar approach with H.R. 3378.

Enforcement of this legislation would also be difficult because the language of Section 101(g) is too vague to provide the judiciary with meaningful guidance in interpreting the exceptions. The bill does not attempt to define or clarify which electronic communications or communications systems are "readily accessible to the general public." Nevertheless, this phrase is the linchpin of the provision and is critical to determining the meaning and scope of Section 101(g).

D. Public Demand

The potential for First Amendment harm, overreaching of the provision, and difficulty of enforcement raises the question of whether Section 101(g) is not in fact overly paternalistic to the American people. Substantial privacy provisions exist in the form of the current wiretapping statutes and Section 701 of the 1934 Act. Although the potential dangers H.R. 3378 attempts to address do exist, there has been no public outcry, other than from cellular telephone interests, demanding government to respond. Indeed, significant efforts have been undertaken in the past by government and others to inform the public of the potential danger of invasion of privacy by the use of the telephone. For example, in the mid 1970's, Vice President Rockefeller made several public statements regarding the potential for eavesdropping on our telephone conversations.

Later in that decade, President Carter also informed the public that the privacy of their telephone calls was subject to being invaded.

In 1978, Sentry Insurance Company obtained the services of the Lou Harris Company to conduct a survey of the American people regarding their views and attitudes toward privacy. The survey results indicated that 9% of the American people polled believed that their telephone calls were not secure and, in fact, almost 10% of the American people who responded believed that their telephones had been tapped. Moreover, they believed that the greatest violator of their telephone security was the U.S. Government, not other individuals.

Notwithstanding the fact that the public has been warned by the nation's highest public officials regarding the lack of security of their telephones and the evidence that that message has been received and understood by the American people, there has still been no hue or cry for additional protection. Considering the cost to other values by an overly broad and potentially dangerous provision such as Section 101(g), Uniden submits that it may be wiser to adopt a course that is designed to provide the American people with the information about the security of their telephone calls and the technology necessary to make individualized choices about protecting their telephone calls.

There is no serious question, and the Committee has heard testimony from others to the effect that a vibrant nascent protection industry is underway which provides a variety of sophistication in cellular protection devices at various costs to cellular and other telephone users. With such technology available, users can select a level of security for their telephones which is commensurate with the economic value they place on the telephone messages they are likely to transmit.

## E. Alternative Legislative Approach

Uniden submits Section 101(g) is an inappropriate and uneffective means of obtaining improved security of radio communications. Uniden, however, believes there is an alternative approach to solving the problem of cellular interception which includes a combination of technology and legislation.

Although the enforcement problems inherent in H.R. 3378 do not negate the need for reform of the wiretap and eavesdropping laws, by clarifying the terms of the bill, and moving the focus to intentionally deciphering a technologically protected message, Congress could alleviate many of the enforcement problems and still achieve the objectives of the reforms. In addition to defining "readily accessible to the general public," the bill should also establish criteria upon which to protect communications. In its present form, the bill does not place any incentive for protection of a message upon the telephone user.

H.R. 3378 should provide users of cellular telephones with incentives to protect their communications. The two most common means of protecting these conversations are by scrambling or encrypting the messages. As Richard Colgan of the Association of North American Radio Clubs demonstrated, voice inversion protection is an inexpensive, effective means of protecting cellular communications. Furthermore, digital encryption provides another, more sophisticated, method of protection.

While the market for scramblers and encryption devices may be in the infant stages, the technology is available and the market is in a position to respond to consumer demands. In the future, more and more messages will be transmitted by digital techniques because of convenience and cost effectiveness. These techniques can make it virtually impossible for casual or inadvertent listeners to intercept private messages.

Legislation should seek to encourage this industry and capitalize on its ability to provide real security to radio communications. Instead, as H.R. 3378 is now written, the progress of this industry will be undercut because the public will have an unfounded expectation of privacy based on an unenforceable statute. This is particularly egregious considering that the encryption industry is developing in an area where the U.S. has clear leadership in the international market, and that market could be stunted by the present legislation.

By placing the burden of protection on the cellular user, the legislation would parallel the marketplace approach adopted elsewhere in radio regulation. Consumers can decide for themselves how much money to spend to protect their communications. Some cellular users may determine that an inexpensive encryption device is sufficient for their needs, while others may require very elaborate, more expensive, protection systems. In either case, the individual, not the Congress, should determine the appropriate level of protection.

For example, the FCC requires that all cordless telephone manufacturers provide prospective purchasers information regarding the security features available on each model. This requirement allows the consumer to make an informed decision about the security of their telephone conversations. Moreover, the FCC has dealt with the same problem addressed by H.R. 3378 in the cordless telephone product line. In adopting Section 15.236 of its Rules, the FCC determined that it was entirely adequate for a notice to be adhered to the telephone which simply states that: "Privacy of communications may not be ensured when using this phone." No public outcry or reaction has occurred. Uniden is at a loss to understand why, if this solution has proven entirely adequate to the cordless telephone product line, a similar solution is not fully adequate for cellular telephones. The principal and utility of the product is virtually the same, and privacy protection devices may be attached to either.

While every encryption technique has the potential to be broken, some of the more sophisticated systems available even today would require the resources of the National Security Agency to unravel. In situations where even these sophisticated systems do not provide adequate protection because the material transmitted is of such a sensitive nature, then whether such data should be transmitted by radio in the first place becomes highly questionable and at some point common sense must prevail. In any event, security will ultimately be determined by the marketplace, not by a flat statutory prohibition of interception.

By placing the initial impetus for privacy protection on the user of the cellular telephones, the bill would establish criteria upon which courts could rely to enforce the law. While there would still be the problems of proof outlined above, there would be fewer problems interpreting the scope and meaning of the bill. In addition, by making scrambling or encryption the standard for enforcement, H.R.

3378 would parallel Section 705(b) of the 1934 Act which protects against interception of encrypted transmissions. Section 705(b) of the 1934 Act places the initial burden of protection upon the satellite broadcaster to protect its transmission. This provision reaches the appropriate balance between First Amendment freedoms and privacy concerns and provides clear guidelines to those government entities responsible for enforcement. Congress should seek a similar resolution of the First Amendment rights and the privacy concerns presented by this legislation.

## III. CONCLUSION

In summary, Uniden supports the concept and the purpose of H.R. 3378. However, in its present form, the bill impermissibly infringes upon the First Amendment rights of the American public and creates confusion with respect to its scope and the mechanics of its enforcement. These effects may have far-reaching consequences which were never intended by the bill's authors. By clarifying the exceptions contained in Section 101(g) and by placing the initial impetus for privacy protection on the cellular user, Congress would achieve the objectives of the bill without placing the ominous burden of interpretation on the judiciary and without placing the cost of enforcement on society as a whole.

# PACIFIC TELESIS GROUP'S RECOMMENDATIONS FOR AMENDMENTS TO H.R. 3378 - THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985

## Title I - Title 18 and Related Matters

1. In Section 101 (b), "Section 2511(2)(g)(i)" should be amended to read:

> "(i) to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is intended to be readily accessible to the public."

This amendment is required to avoid arguments over whether cellular services are "readily accessible to the public" and to ensure that the privacy provisions of the bill pertain to such services.

2. In Section 103, "Section 2520(d)" should be amended to read:

> "(d) A good faith reliance on a court warrant or order, or the request of an investigative law enforcement officer pursuant to Section 2518(7), is a complete defense against a civil action under this section."

## Title II - Pen Registers and Tracking Devices

1. "Section 3121(b)" should be amended to read:

> "(b) EXCEPTION - The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic communication services relating to the operation, maintenance, and testing of an electronic communication service or to protect such provider, or a user of that service, from abuse of service."

2. "Section 3122(a)(3)" should be added and should read as follows:

> "(3) A Federal or State law enforcement officer may not apply for an order to an electronic communications service provider or common carrier requiring such provider or carrier to install and use a pen register."

This language would avoid circumvention of the bill by obtaining an order requiring installation by a telephone company. The bill currently presupposes that the law enforcement officer is obtaining an order to install a pen register himself (with the provision of whatever service is necessary). See "Section 3123(b)(1)(E)". However, in California, courts have been issuing trap and trace orders directly to Pacific Bell. This problem could also be remedied by adding the words "by such officer" after the words "installation and use" in "Sections 3122(a)(1) and (2) and Section 3123(a)" of Section 201(a).

3. "Section 3123(b)(2)" should be amended to read:

> "(2) shall direct, upon the request of the applicant, the furnishing, as is reasonably possible, of information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register or tracking device under section 3125 of this title."

4. The following sentence should be added at the end of "Section 3123(d)":

> "Such person has no obligation to disclose the existence of a pen register or tracking device at any time."

5. "Section 3125(a)" should be amended by adding the words "and as is reasonably possible" after the words "shall furnish such law enforcement officer forthwith".

6. "Section 3128 (c)" should be amended to read:

> "(c) A good faith reliance on a court warrant or order, or the request of a law enforcement officer pursuant to Section 3124, is a complete defense against a civil action under this section."

7. "Section 3129(3)(B)" should be amended either by deleting the words:

> "authorized by a statute of that state to enter orders authorizing the use of pen registers and tracking devices in accordance with this chapter."

or by adding the following sentence:

> "No state court shall issue orders authorizing the use of pen registers and tracking devices unless a state statute expressly authorizes such court to issue such orders."

Such language would avoid a problem which has arisen in California. Although "Section 3129(3)(B)" presupposes that a specific state statute will expressly give authority to issue pen register orders, no such statute exists in California. Nevertheless, courts have recently issued such orders in San Francisco and Santa Clara, apparently on the basis of very broad statutory authority of courts to do what is needed in the interest of controlling the criminal justice system when there is no specific rule covering a situation. It has been generally assumed that such statutes give the courts such authority, but the issue is far from clear. Since this bill deals with the subject, it should clarify the issue.

## Statement of
## The National Association of Business and Educational Radio
## Concerning
## The "Electronic Communications Privacy Act of 1985"

The National Association of Business and Educational Radio, Inc. ("NABER") is a national non-profit association formed in 1965 which represents over 5,000 member companies and individuals who hold hundreds of thousands of licenses issued by the Federal Communications Commission to operate radio systems in the Business Radio Service and in the other Private Land Mobile Radio Services. NABER's membership includes both large and small companies who are licensees in the Business Radio Service and who use radio communications as an important adjunct to the operation of their businesses. In addition, NABER's membership includes manufacturers and vendors of products and services in the Private Land Mobile Radio Services as well as hundreds of Specialized Mobile Radio Service licensees who provide service to radio users as private carriers.

Encouraging the efficient and compatible use of the electromagnetic spectrum has been one of NABER's primary concerns and goals as an organization. Since its inception, NABER has had a continuing involvement on a nationwide basis with the problems and spectrum needs of existing and future Business Radio Service licensees as well as other Land Mobile Radio users and service providers. Furthermore, NABER is the FCC recognized frequency coordinating committee for the Business Radio Service.

There are numerous types of Private Land Mobile Radio systems designed to meet the specific communication requirements of various users. Systems may vary in range and in size from an extensive regional operation or even a nationwide system needed to serve the particular internal communication needs of a large corporation, to the more typical local system serving a small business concern. The many kinds of communications for which private systems are utilized include voice, data, tone or a combination thereof. In addition, private land mobile systems may be two-way, one-way, radio dispatch or mobile telephone service. The Federal Communications Commission estimates that, as of 1984, there are approximately 950,000 authorized stations using nearly eight (8) million transmitters in the Private Land Mobile Radio Services which have an annual growth rate of 6.5%. 1/

In order to accommodate demand for frequencies by Private Land Mobile Radio users, the allocation of frequencies in the Private Radio Services has been generally made on a non-exclusive and shared basis. That is, users in the Private Land Mobile Radio Services are on the whole required to share frequencies and to cooperate with one another in order to resolve any interference problems. Further, in order to assist and to encourage

---

1/ Notice of Proposed Rule Making, PR Docket No. 84-1233, 50 Fed. Reg. 1582 (Jan. 11, 1985).

efficient utilization of the frequencies, licenses are issued in the private services only to those applicants who are eligible in such services and who will use such frequencies only for permissible communications on such systems. For example, in the Business Radio Service, licensees and users must be primarily engaged in the operation of: a commercial activity; an educational, philanthropic or ecclesiastical institution; clergymen activities; or hospitals, clinics or medical associations, and use of such frequencies are limited to only communications which are adjunct to such activities.

It is NABER's view that the proposed Electronic Communications Privacy Act of 1985 (S.1667) would inadvertently include into its gambit otherwise normal and acceptable operational activities conducted on Private Land Mobile Radio systems. Such a result would therby restrict what has to date been considered a normal and acceptable mode of operation. Specifically, since private radio frequencies are oftentimes shared and in heavy use, the only means to ascertain whether or not a particular frequency is the best frequency available requires monitoring of other users on that frequency prior to application with the Federal Communications Commission. Further, shared systems in the Private Land Mobile Radio Services in their normal operation necessarily involve a user who will monitor a shared frequency to demonstrate when it may be accessed in order to initiate communications. In addition, base station operators may also monitor communications over their systems for control purposes as well as to insure efficient use of the spectrum. Finally, in the private radio services, technical difficulties or interference concerns arise which require the monitoring of other systems in order to ascertain the possible source or cause of such interference. NABER's concern is that in the Private Land Mobile Radio Services, particularly when frequencies are shared and used on a non-exclusive basis, radio users do not have the same expectations of privacy as anticipated in the Bill which would override the normal functioning of their communication system. Further, even in the instance of exclusive allocations, the base station licensee may have a technical necessity to monitor users on his system, particularly where such users are his employees or otherwise under his control.

NABER is further concerned that the Bill's substitution of the definition of "communication common carrier" and the insertion of "a provider of electronic communications service" would include private carrier licensing in the Private Land Mobile Radio Services which by statute, regulation, and historical operation has been distinct from that of common carriage. In this respect, the Commission has provided that the Private Land Mobile Radio Services are governed by Part 90 of the FCC Rules whereas Common Carrier service is regulated under Part 22. Further, in the Private Land Mobile Radio Services, frequencies are generally made available for particular classes of eligibles, rather than for providers of radio services ("common carriers") who offer such services indiscriminately to the general public.

October 25, 1985

## ANALYSIS OF H.R. 3378 (Same as S. 1667)
## "ELECTRONIC COMMUNICATIONS PRIVACY ACT of 1985"

### §101(a)(1)

This subsection would strike the present definition of "wire communication" in 18 U.S.C. §2510(1) and substitute therefor a new, broader definition of "electronic communication." Whereas the present definition simply refers to "any communication," the new definition would include "any transmission of signs, signals, writing, images, sounds, data, or intelligence of any nature." Furthermore, while the present definition speaks of communications "in whole or in part...by the aid of wire, cable, or other like connection," the new definition would encompass transmissions "by a wire, radio, electromagnetic, or photoelectric system." Finally, unlike the present definition, the new definitions would not be limited to facilities "furnished or operated...by a common carrier." Thus, the new definition would make clear the Congressional intent that the law protect data as well as voice communications (and remove any lingering question about its applicability to digitized voice communication), would not require that any part of the communication be by wire, cable or the like (as might be the case, for example, in certain radio transmissions), and would extend the protection of the statute to transmissions over private communication systems as well as common carrier facilities.

__§101(a)(2)__

This subsection would strike the words "aural acquisition" from the present definition of "intercept" in 18 U.S.C. §2510(4) and substitute therefor the word "interception." Deletion of the word "aural" would eliminate the basis upon which the existing law has been interpreted as not covering data communications. This, in conjunction with the proposed, new definition of "wire communications" should make absolutely clear that data communications are to be within the scope of the amended statute. However, the substitution of "interception" for "acquisition" seems to be an attempt to define a term by a derivation of that same term and calls, in turn, for a definition of the latter. While the use of "acquisition" apparently has not caused problems in applying the law to voice communications, this bill would extend that coverage not only to data communications but to data stored in a computer. In that regard, it may be that the draftsmen of the bill were concerned that "acquisition" connoted some taking of possession, a concept which has proven troublesome in attempts to apply the principles of common law larceny to theft of data from a computer. If that is the case, perhaps the definition could be rephrased as "the acquisition, reception, detection or recording of the contents...."

__§101(a)(3)__

This subsection would strike the word "existence" from the definition of "contents" in 18 U.S.C. §2510(8). The result is that divulgence of the mere existence of a communication, or endeavoring to use that information, knowing such information was obtained through an unauthorized interception, would not violate the statute. (See 18 U.S.C. §§2811(1)(c) and (d).) This is seemingly consistent with other provisions of the bill (see §101(b) below) which provide that it shall not be unlawful to use a pen register, or for a provider of electronic communications service to record the "placement" of a telephone call to protect itself, its users and its service from abuse. However, it also seems to create a divergence from the language of §705 (formerly §605) of the Communications Act (47 U.S.C. §705(a) as redesignated and amended by §§5 and 6(a) of P.L.98-549), which provides that persons involved in transmitting or receiving interstate or foreign communications by wire or radio shall not divulge "the existence, contents, substance, purport, effect or meaning thereof."

§101(b)

This subsection would create several exceptions, in addition to those already listed in 18 U.S.C. §2511(2), to the prohibition against interception set forth in §2511(1). Included are communications transmitted: (1) over systems designed to be readily accessible to the public; (2) for use of the general public relating to ships, aircraft, vehicles or persons in distress; (3) by walkie talkie, or police and fire communications systems readily accessible to the public; and (4) by amateur radio station and citizens band radio operators.

While in some cases (*e.g.*, certain police or fire communications) it may be appropriate to limit the exception to interception of the communication, in other cases (*e.g.*, distress calls) the exception should also include disclosure and use of the information obtained.

This subsection would also provide that it shall not be unlawful, for the purposes of Ch. 119 of Title 18, dealing with interception of wire - "electronic" under the bill - and oral communications), to use a pen register as defined in a proposed, new Ch. 206 of Title 18 (but see the restrictions on such use in that Ch. 206 as described under §201(a) below.) Also, for the purposes of Ch. 119, it would not be unlawful for the provider of an electronic communication service to record the placement of a telephone call to protect itself, its users and its service from abuse. While "abuse of service" is not defined, its meaning is probably well enough established in the telecommunications industry to encompass obscene or harassing calls and toll fraud. However, this protection against "abuse of service" under Ch. 119 should be compared with the inadequate protection afforded in connection with the use of pen registers under the proposed Ch. 206 (see §201(a) below.)

**§102(a)**

This subsection would add new prohibitions to those already established in 18 U.S.C. §2511(1) against the interception of communications and the disclosure or use of information so obtained. The new provisions would proscribe wilfully, without authorization, accessing an "electronic communications system," or wilfully exceeding any access authorization, and obtaining or altering an electronic communications stored in the system. While the obvious intent is to include computers and their data bases within the meaning of "electronic communication system," that term is not defined in the bill, and that result is not assured. A narrow interpretation could limit "electronic communication system" to means of transmissions, rationalizing the use of the phrase "stored in such system" as a reference to so-called store-and-forward transmission services. To obviate this potential, "electronic communication system" could be defined in §101 of the bill, perhaps as "any means of transmissions, reception, processing, storage, retrieval or retransmission of electronic communications."

The penalties for violating these provisions could be severe (i.e., fines up to $250,000, imprisonment up to one year for the first offense, two years for subsequent offenses, or both) if the offense were committed for purposes of commercial advantage, malicious destructions or damage, or private commercial gain. In all other cases, the penalties could be much less (i.e., fines up to $5,000, imprisonment up to six months, or both.) This seems to reflect the continuing concern of some legislators that teenage "hackers" and the like, whose motivation is not commercial or malicious, should not be penalized too severely. However, even the activities of such "hackers" have the potential of causing great harm to others (e.g., denial of legitimate use of computer facilities or inadvertent disclosure of proprietary information.) There is a serious question whether such consequences (i.e., denial of use or disclosure of data) are within the prohibitions of this subsection of the bill which would apply to anyone who "obtains or alters" an electronic communication. There is a further question whether the civil remedies in 18 U.S.C. §2520, which refers to persons whose communications are "intercepted, disclosed, or used" (the bill would add "accessed," see § 103 below) in violation of the law, would provide any relief in such circumstances. Certainly this proposed amendment needs to be revised so as to prohibit not only unauthorized access (or access in excess of authorization) but also "obtaining, using, disclosing, altering, damaging or destroying electronic communications stored in such system, or denying access to, or use of, such electronic communications, or the system in which it is stored, to authorized users."

Subsection 102(a) of the bill would also prohibit the provider of an electronic communication service from knowingly divulging the "contents" of any communication carried over that service (other than one to such provider) to other than the addressee or addressee's agent, except: (1) as authorized by court order; (2) with the consent of the originating user; (3) to persons employed to forward such communication; or (4) "for a business activity related to a service provided by the provider of the electronic communication service to a user of the electronic communication service." The scope of this last exception is unclear. Presumably, it is intended to apply to a data processing service or something of that nature. However, the language used ("a business activity" could be almost anything, "related to a service" could be very tangential, "provided...to a user" need not be the originator or addressee of the particular communication) could be construed to encompass situations where divulgence of the "contents" could well be deemed improper. Without knowing exactly what is intended, it is not really feasible to suggest amendatory language. However, it might be that a slight change in the proposed exception for originator consent, to read "consent of the user originating, or the addressee, of such communication," would cover the intended situations while providing adequate safeguards.

As noted above (see §101(a)(3)), divulgence of the "contents" would not, under the definitions of that term in this bill, proscribe divulgence of the "existence" of a communication.

§102(b)

This subsection would add two new provisions to 18 U.S.C. §2516, the section of the law which empowers certain law enforcement officials to authorize applications for court orders to intercept communications. The first of the new provisions would empower the same officials to authorize applications for disclosure which would otherwise violate the new prohibitions to be added to 18 U.S.C. 2511 by the bill (see §102(a) above.) But as already discussed, the new prohibition against unauthorized accessing of stored data does not expressly proscribe disclosure. The ambiguity of scope of the exception (for related business activity) to the other new prohibitions to be added to 18 U.S.C. 2511 has also been discussed above.

The second new provision in §102(b) of the bill would forbid the provider of an electronic communication service from disclosing, upon request of a governmental authority, any record kept in the course of providing that service and relating to a particular communication over that service, unless the governmental authority obtains a court order for such disclosure based on findings of reasonable suspicion that the party making or receiving that communication is engaged in criminal conduct and that the record sought contains information relevant to that conduct. The obvious intent here seems to be the protection of toll billing records from government snooping, or even legitimate investigation without judicial scrutiny. While this intention may be noble, the absolute prohibition contained in the proposed legislation seems to go beyond the necessary or appropriate limits of such a provision. At a minimum, there should be some exceptions to this prohibition, e.g., permitting disclosure without a court order with the consent of the party making the particular communication, to employers or agents of the service provider in the ordinary course of conducting that communications business, in emergency situations where life or property may be in jeopardy, or where the particular communication represents an abuse of service or violation of law. Also, if a prohibition of this nature, even one more narrowly circumscribed, is appropriate for governmental agencies, is it not equally appropriate for private parties whose interest in such records may be more personal or otherwise less legitimate?

§103

This subsection would amend 18 U.S.C. §2520, which provides civil remedies for interception, disclosure or use of communication in violation of the statute, to add unauthorized access as a basis for recovery. The amendment would also: (1) provide for preliminary, equitable or declaratory relief; (2) add to the actual damages recoverable "any profits made by the violator;" (3) change the provisions for statutory damages from $100 a day or $1000, whichever is higher, to not less than $500 nor more than $10,000; (4) delete from the "good faith reliance" defense reliance on "legislative authorization;" (5) exclude all criminal actions from the scope of that defense; (6) eliminate that defense for civil actions brought "under any other law;" and establish a two year statute of limitations for civil actions based on violation of this statute.

There appears to be some troublesome aspects to these proposed changes. For example, does it make any sense to grant a complete defense against civil actions under this statute (i.e., Ch. 119 of Title 18) but not under other laws. If the same conduct is actionable under two different statutes and a defense is granted only by one, that grant may be meaningless. Similarly, is there any good reason from granting a complete defense against civil actions but making that same conduct, motivated by reliance upon the same court order which gives rise to civil immunity, subject to possible criminal penalties. Of course, when the elements of the offense include a wilful act with knowledge or reason to know that such conduct would violate the statute, a "good faith reliance" defense would be superfluous. But, in some instances, the essence of the offense is only a wilful act not otherwise authorized by the statute (i.e., pursuant to a court order.) This raises another question, applicable both to the present law and the proposed changes. In order to receive the benefit of the statutory good faith defense, can reliance be placed upon a court order "valid on its face," or must that order, in fact, be "valid." Frequently, there may be no way for laymen or even lawyers to determine, before a response is required, whether there has been some defect in the procurement of a court order and, if so, whether that defect is of such a nature as to invalidate the order. In such circumstances, the person served with the order is put on the horns of a dilemma: comply with the order, and risk civil damages and criminal penalties if the order is later determined to be invalid, or refuse to comply and risk being charged with contempt of court if the order is later held to be valid. This dilemma should be eliminated by the language of the statute.

§104

This section would add and "acting Assistant Attorney General" to the list of federal law enforcement officials empowered to authorize applications for court orders under 18 U.S.C. §2516(1).

§105

This section would add some new crimes to the list of offenses in 18 U.S.C. §1516(1)(c) for the investigation of which federal law enforcement officials are authorized to seek court orders. Of particular interest to us is the addition of 18 U.S.C. §1029 dealing with fraud and related activities in connection with access devices (which, as defined in §1029(e), includes AT&T Calling Cards.)

§106

This section would amend various parts of 18 U.S.C. §2518, which sets forth the procedures for interception of wire ("electronics" under the bill) or oral communications. It would: (1) require that applications for court orders identify specific investigative objectives and targets, if known (§2518(1)(b)); (2) list several alternatives investigative techniques (including use of pen registers) as to which the application must state whether they were tried and failed or why they appear unlikely to succeed or to be too dangerous (§2518(1)(c)); (3) permit interception to take place outside the territorial jurisdiction of the court issuing the order in the case of a mobile intercept device installed within that jurisdiction (§2518(3)); (4) change the basis of compensation for court mandated furishing of "information, facilities, and technical assistance" from "prevailing rates" to "reasonable expenses" (§2518(4)); (5) empower courts to authorize physical entry to install an interception device when no less intrusive means of interception is reasonably available, but no court order would require participation by operators or employees of electronic communications systems (added to §2518(4)); (6) make mandatory periodic reports to the court concerning progress towards authorized objectives and the need for continued interception (§2518(c)); and (7) grant law enforcement authorities up to 48 hours after expiration of an order to make recordings of interceptions available to the judge who issued that order (§2518(8)(a)). The principal concern with these proposed amendments arises from the prohibition against requiring operators or employees of electronic communication systems from participation in a physical entry in order to install an interception device. While we certainly do not want to be involved in any such activity, the implication seems to be that, in situations not requiring physical entry, we can be required to participate in actually "effecting the interception." To date, we have taken the position that the "technical assistance" we may be required to render under court order under this statute is limited to advice and does not include any participation (beyond making a cross-connection in a Central Office) in effecting the interception. Of course, in the post-divestiture environment, this is really a concern for the LECs rather than AT&T.

Another possible concern arising from these amendments is the requirement that law enforcement authorities consider and utilize alternate investigative techniques before resorting to interception. The result may be a significant increase in request for assistance to install pen registers (see §201 below) to satisfy the statutory requirement followed by requests for assistance with interception, the investigative technique which the law enforcement authorities really wanted to use from the outset of their investigation.

§107

The section would shorten the interval, from every four years to every year, at which the Foreign Intelligence and Surveillance Act (see 50 U.S.C. §1808(b)) would require House and Senate Committees on Intelligence to report to the House and Senate, respectively, concerning the implementation of that Act.

§108

This section would establish the effective date of the foregoing amendments (*i.e.*, 90 days after enactment and, for conduct pursuant to court order, only with respect to orders or extensions granted after that date.)

§201

This section would insert a new Ch. 206 in Title 18, to govern the use of pen registers and tracking devices. The new Chapter would consist of nine sections, number 3121 through 3129, as follows:

> §3121 - subsection (a) would prohibit any installation or use of a pen register or

tracking device without a court order. Subsection (b) would provide an exception to this prohibition for "use of a pen register by a provider of communications services relating to the operation, maintenance, or testing of an electronic communication service." This exception is inadequate and could seriously impair legitimate activities by providers of such services to protect their assets and revenues. The exception should be expanded to read "operation, maintenance, testing and protection against fraud and abuse" of the service. Compare the exception the bill would create in Ch. 119 for "a provider of electronic communication service to record the placement of a phone call in order to protect such provider, or a user of that service, from abuse of service" (see §101(b) above.) Provisions for use of pen registers or tracking devices, without court order, in emergency situations are covered in another section of the proposed new Ch. 201 (see §3124 below.) Subsection (c) would provide for fines up to $100,000, imprisonment up to a year, or both, for knowingly violating the prohibition against use of a pen register or tracking device without a court order.

§3122 - subsection (a) would authorize federal and state law enforcement officers having responsibility for an ongoing criminal investigation to apply for a court order. Subsection (b) covers the contents of an application for such an order. The requirements are much less stringent than for an order authorizing interception under Ch. 119. All that would be needed is the identity of the applicant and his law enforcement agency, and "a statement of the facts and circumstances relied upon...to justify...belief that an order should be issued."

§3123 - subsection (a) would authorize the court to issue an ex parte order authorizing use of a pen register or tracking device (outside the territorial jurisdiction of the court in the case of a mobile tracking device installed within such jurisdiction) if there is reasonable cause to believe (in the case of a pen register) or probable cause to believe (in the case of a tracking device) that information so obtained would be relevant to a "legitimate criminal investigation." Although §3122(a)(2) of the new Ch. 206 would expressly empower state law enforcement officers to apply to state courts for orders authorizing use of pen registers and tracking devices, the phrase "legitimate criminal investigation" is defined in the new Ch. 206 (see §3129(4)) as an investigation "into a violation of any Federal criminal law." If state law enforcement officers are meant to be empowered to apply for court orders, surely it must be intended to include investigation of violations of state criminal law as well. Perhaps the best solution would be to change the word "legitimate" to "ongoing," a term already used in §3122, and simply delete this confusing definition. If violations of state law are included, there is also a question whether all states have laws making obscene, harassing or nuissance calls criminal? If they do not, then court orders could not be obtained and pen registers could not be used in those non-criminal situations. The different standards for issuance of court orders for use of pen registers and tracking devices probably reflects the differences in the degree of intrusiveness and expectation of privacy involved.

Subsection (b) of §3123 covers the contents of court orders authorizing use of pen registers or tracking devices. Included, in the case of pen registers, would be the telephone number of the line and the identity of the subscriber or a person "who commonly uses the telephone line." The order could also direct the furnishing of "information, facilities, and technical assistance" to "accomplish the installation and use of the pen register." Here, presumably, the equipment would be owned and operated by the LECs.

Subsection (c) would limit the use of pen registers or tracking devices, pursuant to court order, to the period necessary to achieve the objective of the authorization, not to exceed 30 days. However, extensions, not to exceed 30 days each, could be obtained.

Subsection (d) of §3123 would provide that the court order may require the person owning or leasing a telephone line to which a pen register is attached, or assisting in its installation and use, not disclose its existence until at least 60 days after its removal. There could be extensions of not more than 60 days each upon a showing of reason to believe that disclosure would endanger life or physical safety, result in flight from prosecution, destruction of (or tampering with) evidence, intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or governmental proceeding.

§3124 - subsection (a) would permit a law enforcement officer "specially designated by the Attorney General" to install or use a pen register or tracking device without a court order provided that (1) "a judge of competent jurisdiction" is notified when the decision is made; (2) the law enforcement officer reasonably determines that an emergency situation exists (involving immediate danger of death or serious injury, or conspiratorial activities threatening national security or characteristic of organized crime) that requires use of the device before an order could be obtained; (3) the law enforcement officer reasonably determines that there are grounds upon which an order could be obtained; and (4) an application for an order will be made within 48 hours. This provision differs somewhat from that in Ch. 119 authorizing interception of wire ("electronic" under the bill) or oral communications. In the latter case, there is no express exception for emergency situations involving danger of death or serious injury. On the other hand, that provision includes law enforcement officers specially designated by "the principal prosecuting attorney of any state or subdivision thereof." Surely, if the state law enforcement officers can apply for state court orders in the investigation of state crimes, the emergency exception for use of pen registers and tracking devices also should be extended to state authorities. The reference to a "judge of competent jurisdiction" seems to be and editorial oversight. The reference seemingly should be to a judge of a "court of competent jurisdiction," which is a term defined in the proposed new Ch. 206 (see §3129(3) below.) However, the phrase "judge of competent jurisdiction" is also used (and defined) in Ch. 119 (see §2510(9)). Subsection (b) of §3129 would provide that use of a pen register or tracking device in an emergency situation without a court order "shall terminate immediately when the information sought is obtained, or an application for the order is denied, whichever is earlier." No provision is made regarding disposition of information obtained by use of a pen register or tracking device when the application for an order is denied. Similarly, no provision is made concerning use as evidence of information obtained in violation of the new Ch. 206.

3125 - this section expands upon the earlier provision, relating to the content of court orders (see §3122(b) above), regarding the furnishing of "information, facilities, and technical assistance." Subsection (a) of §3125 mandates such assistance by "a communications common carrier, landlord, custodian, or other person," when directed by a court order or in connection with the exception for emergency situations. If the carrier actually installs and operates a pen register, it must really act at its peril in rendering assistance in an emergency situation. Not only is there no order upon which to rely, but also there is no way really to determine whether the law enforcement officer has a reasonable basis for acting without an order.

Subsection (b) of §3125 would prohibit law enforcement officers from requesting participation by operators or employers of electronic communications systems "in such physical entry." The use of the word "such" implies some antecedent, but the proposed new Ch. 206 would not, as would the amended Ch. 119 (see §106(d) above), expressly authorize "physical entry" by law enforcement officers.

Subsection (c) of §3125 would provide for compensation "for reasonable expenses incurred" in providing facilities or assistance to law enforcement officers.

§3126 - subsection (a) would require that, within 90 days after expiration or denial of an order, the issuing or denying judge "shall cause to be served" on the persons named in an application or order, or whose activities were monitored by the pen register or tracking device, "an inventory" to include notice of the application or order, the date the order was approved or denied, and the period of time that activity took place under the order. Although the bill uses the word "inventory" the requirement seems to be more in the nature of a "notice." From the language used, it is not clear whether this provision puts the onus of providing notice on the government, or whether a judge could, for example, order a carrier to give notice to its subscriber about use of a pen register in which the carrier assisted.

Subsection (b) of §3126 would permit "a judge of competent jurisdiction" (see comment under §3124(a) above), on a showing of good cause, to postpone service of the inventory, or to dispense with it if such notice would compromise an ongoing criminal investigation or would result in disclosure of classified information harmful to national security.

Subsection (c) of §3126 would permit a judge, upon motion, to make available for inspection by a person or his counsel such applications, orders and results of activity under orders as the judge, in his discretion, determines to be in the interests of justice.

§3127 - subsection (a) would require reports by judges issuing or denying orders for use of pen registers and tracking devices to make certain reports to the Administrative Office of the United

States Courts. Subsection (b) would require annual reports to the same office by the Attorney General, or a specially designated Assistant, and principal prosecuting attorneys of states and political subdivisions, on the results of using pen registers and tracking devices. Subsection (c) would require the Director of the Administrative Office of the United States Courts to file annual reports with Congress, which would include summaries of the information reported under subsection (a) and (b).

§3128 - subsection (a) would provide a civil cause of action to anyone "harmed by a violation of this chapter." Subsection (b) would provide for preliminary, equitable or declaratory relief in such an action, as well as recovery of damages, attorney's fees and costs of litigation. Subsection (c) would make good faith reliance on a court warrant or order a complete defense to such a civil action. And, subsection (d) would establish a two-year statute of limitations for such actions.

§3129 - this section would define various terms used in the proposed new Ch. 206. Other than as already discussed above, the only significance of this section from our point of view is the definition of a pen register as "a device which records and or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on a telephone line." That term would not include "any device used by a provider of electronic communications services for billing, or recording as an incident to billing, for communications services provided."

## §202

This section provides that the new Ch. 206 would take effect on the date of enactment.

John R. Davis

AT&T
Suite 1000
1120 20th Street N.W.
Washington, D.C. 20036

Submitted by: Terry Banks

October 17, 1985

COMMENTS OF H. W. WILLIAM CAMING, ATTORNEY AND CONSULTANT,
UPON
THE " ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985 " ---
H.R. 3378 ( AS INTRODUCED BY MR. KASTENMEIER ) AND S. 1667
(AS INTRODUCED BY MR. LEAHY) ON SEPTEMBER 19, 1985.

( Since 1965, Mr. Caming has been the senior counsel at American Telephone & Telegraph Company specializing in, and having legal oversight over, matters pertaining to privacy, information technology, corporate security, and criminal law as they affected AT&T and its affiliated Bell System entities. He also served as the Company's principal spokesman on such matters before Congress and other legislative and regulatory bodies, and with the press. Mr. Caming retired on October 1, 1984 to act as an attorney and independent consultant in these areas. )

*************************************

### 1. Section 101(a)(1); Definition of "Electronic Communication"

It is suggested that this definition be revised as follows:

(1) ' electronic communication' means any communication made in whole or part through the use of facilities for the transmission of signs, signals, writing, images, sounds, data, or intelligence of any nature (~~in-whole-or-part~~) by a wire, radio, electromagnetic, or photoelectric system that affects interstate or foreign commerce where the person originating such communication exhibits an expectation that such communication is not subject to interception under circumstances justifying such expectation.

Legends:

| | | |
|---|---|---|
| As used herein, | __________ | Underlining denotes addition to text. |
| | (~~-whole-~~) | Parenthetical language dashed out denotes deletion of text. |

Commentary:

(1) The suggested additional language, "communication made in whole or part through the use of facilities for the," is consonant with the existing definition of "wire communication" in Sec. 2510(1) of Title III and stresses that the means of communication and not the content are being regulated. Thus, judicial interpretations over the past 15 years will have continuing application and First Amendment issues, to the extent applicable, will be minimized.

(2) The expectation of privacy language added at the end of the definition is consistent with the language currently employed in the definition of "oral communication" in Sec. 2510(2) and U.S. Supreme Court decisions on privacy issues.

### 2. Section 101(a)(2): Definition of "Intercept"

It is suggested that in line 14 on Page 2, the phrase, " or other technological means of interception" be inserted(after the proposed substitution of "interception" for " aural acquisition ") , so that the term 'intercept' would read as follows:

BEST COPY AVAILABLE

'intercept' means the interception (~~aural-acquisition~~) of the contents of any electronic (~~wire~~) or oral communication through the use of any electronic, mechanical, or other device or other technological means of interception.

Commentary:

The additional language will ensure that any radically novel means of technology that may be introduced for the transmission of electronic communications in the future will fall within the purview of this statute. Advances in telecommunications and computer technology have been so great as to warrant the precaution.

3. Need for Definitions of Certain Terms:

Inasmuch as this is a criminal statute, it is suggested that for purposes of clarity and specificity consideration be given to including within the Act a definition for each of the following terms:

-Electronic Communication System

-Electronic Communication Services

-Provider of Electronic Communication Services

-User of Electronic Communication Services

-Access

4. Section 101(b): Exceptions With Respect to Electronic Communications

It is suggested that on Page 3, Lines 6-8, the provision be revised to read as follows:

(II) by a ( ~~walkie-talkie-or-a-~~) police or fire communication system(~~readily~~)accessible to the general public; or

Commentary:

(1) The term "walkie talkie" is a lay term, may be technologically restrictive, and falls within the provisions of Sec. 2511(2)(g)(i) on Page 2, Lines 22-25.

(2) The term "general public" has long been used in Sec. 705(a) of the Communications Act of 1934 (47 U.S.C.).

5.Sec. 102(a): Additional Prohibitions

It is suggested that the new subsection (3) to Sec. 2511 be revised for purposes of clarity in the following two respects:

-Page 6, Line 7 be revised to read as follows:

munication service and obtains (~~or~~) ,alters, damages, or destroys that electronic com-

Commentary:

This addition is more consistent with the language of subparagraph (A) on Page 6, Lines 9-11.

-Page 6, Lines 20 -21 be revised to read as follows:

(B) be fined not more than $5,000 or imprisoned not more than six months, or both, ( ~~in-any-other-case~~ ) if the offense is committed for a purpose other than commercial advantage, malicious destruction or damage, or private commercial gain.

6.Sec. 102(a): Prohibition Against Divulgence of Contents of Electronic Communication - Exception for Business Activity

Sec. 2511 is amended by adding a prohibition against knowingly divulging the contents of any electronic communication, with stated exceptions. One such exception -- Sec. 2511(4)(D), which appears on Page 7, Lines 9-12 -- reads as follows:

> (D) for a business activity related to a service provided by the provider of the electronic communication service to a user of the electronic communications service.

The"business activity" referenced in Paragraph D is not wholly clear as to its meaning. Seemingly, it is covered in exception (B) of Sec. 2511(4) - with the consent of the user originating such communication. I would suggest that the language be clarified in the text and/or appropriate legislative history be included.

7. Sec. 102(b): Requirements for Certain Disclosures

Sec. 2516 of 18 U.S.C. is amended by adding , among others, a subsection 4, which appears on Page 8, Lines 6-18.*It prohibits a provider of electronic communication service from disclosing, upon request of a governmental authority, any"record"kept by that provider relating to a particular communication made through that service, unless the government obtains a specified type of court order for such disclosure ( findings of relevancy to the investigation and reasonable suspicion standard ).

This provision would appear to reach telephone toll billing records maintained by communications common carriers. As I have previously testified, it has been the policy and practice of Bell System Operating Telephone Companies since 1974 to disclose its toll billing records, and related subscriber records, upon presentation of a court order or other lawful process of a governmental authority ( e.g., a grand jury, statutory, or administrative subpoena ). It is my understanding that since divestiture of the Bell Operating Companies, that policy has generally been continued. The requirement for a court order in all instances is more restrictive.

Further,the sole exception to the requirement of a court order or other lawful process by the Bell Companies was in the instance of National Security.

It has been the policy and practice to provide toll billing records, and related subscriber records, upon the specific written request of the Director of the Federal Bureau of Investigation, or of an Associate Director or one of several specifically Designated Assistant Directors of the FBI, for such information for national security purposes, under the Presidential power to obtain foreign intelligence information or to protect the national security against actual or potential attack, hostile acts, or the intelligence activity of a foreign power.

- Accordingly, the Congress may want to review this question with the appropriate Federal intelligence authorities to determine whether a statutory exception of some nature is to be granted in the instance of national security.

---

* All pagination references used herein are to H.R. 3378.

### 8. Sec. 103: Recovery of Civil Damages

It is suggested that the amendatory provisions of Sec. 2520 of 18 U.S.C. include within Sec. 2520(b) a provision for punitive damages - perhaps as Paragraph (3) thereunder - and the present Paragraph (3) on Page 9 at Lines 8-9 relating to attorney's fee and other costs of litigation could be renumbered "(4)".

- Punitive damages have been available as a remedy under Section 2520 since the inception of the Act, to serve as a further deterrent to violation of the Act.

It is further suggested that on Page 9,Lines 10-11 be revised to read as follows, for purposes of clarity and to enhance the deterrent quality of the civil remedy:

> (c) The court may assess as damages in an action under this section whichever is greater of ( ~~either~~ ) --
>
> ....
>
> (2) statutory damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $10,000, whichever is higher ( ~~not less than $500 or more than $10,000~~ )

### 9. Sec. 103: Good Faith Reliance

It is suggested that Sec. 2520(d), which appears on Page 9 at Lines 17-18, be revised to read as follows:

> (d) A good faith reliance on a court warrant or order or on the provisions of section 2518(7) of this chapter shall constitute a complete defense against any ( ~~a~~ ) civil or criminal action brought under this chapter (section).

Commentary:

This provision has been in full force and effect since 1970 ( P.L. 91-358, 91st Cong., July 29, 1970 ). The provision proposed on Page 9 affords no protection against civil suit when assistance of an emergency nature is lawfully provided. Further, protection against criminal prosecution has always been part of the law.

### 10. Sec. 105: Physical Entry Authorized

It is suggested that the provision authorizing an order for physical entry by law enforcement, to be added to Sec. 2518(4) of 18 U.S.C., which appears on Page 12 at Lines 4-12 be revised in part to read as follows:

> (2) by adding at the end " An order authorizing the interception of an electronic communication may ... authorize physical entry by law enforcement officers into any premises ( other than those being used by a provider of electronic communication service to provide such service) to install an electronic, mechanical, or other device....

Commentary:

The proposed prohibition against entry by law enforcement authorities to the Central Offices or other operating premises for purposes of wiretapping or other surveillances is of the longest standing, antedating the Federal Omnibus Crime Control and Safe Streets Act. It reflects uniform Bell System practices of the Operating Telephone Companies which I understand have been continued in this respect after divestiture.

The limited nature of the assistance to be rendered by the communications common carriers has always been recognized and accepted by the Congress. My testimony in behalf of the Bell System for more than a decade has reflected the policy of not permitting law enforcement authorities to enter operating premises for purposes of wiretapping.

### Re: Title II - Pen Registers and
### Tracking Devices

### 11. Sec. 3121: Exception to General Prohibition on Pen Register Use

It is suggested that the Exception in Sec. 3121(b) be revised by amending its provisions to read as follows:

> (b) Exception. - The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic communication services relating to the operation, maintenance, ( and ) testing, and protection against theft or abuse of such service.

Commentary:

This reflects similar treatment under Title III. Communications common carriers regularly are required to use pen registers to protect against theft of its services and to prevent or uncover abuse of its customers' service ( e.g., in annoying call situations ).

### 12.Use of Term, "Law Enforcement Officer".

Throughout Chapter 206 - Pen Registers and Tracking Devices - the term, "law enforcement officer" is used. However, Chapter 119 uses the term "investigative or law enforcement officer" and defines this term in Sec. 2510(7). It is not clear why this latter term was not used in Chapter 206 and what, if anything, in intended by such change in terminology.

At the least, a definition of the term might be included in Chapter 206, with appropriate legislative history if the change is enacted into law.

### 13. Sec. 3123: Issuance of a Pen Register Order

It is to be noted that in the Bell System since the decisions of the U.S. Supreme Court in the leading pen register cases ( U.S. v New York Telephone Company; Smith v Maryland ),limited cooperation was accorded to law enforcement in pen register cases - in the form of cable and pair information relating to the targetted telephone line and a leased line channel between the terminal serving the suspect's line and the terminal serving the listening post of law enforcement - upon the presentation of a Rule 57(b) Federal court order. Such order was issued on the "reasonable cause to believe" standard which is now adopted in this Act on Page 16 at Lines 8-9.

Commentary:

Due to the importance of the use of a pen register device as an investigatory measure in many major criminal investigations and use of the Rule 57(b) Order for a number of years without untoward incident, the "reasonable cause to believe" standard appears to strike a proper balance of the countervailing considerations.

## 14. Sec. 3123: Relevant to a Legitimate Criminal Investigation.

Under Section 3123(a), a pen register order may issue if the information likely to be obtained is relevant to a "legitimate criminal investigation" (Page 16, Lines 12-13).

Section 3122 authorized Federal law enforcement officers in subsection (a)(1) thereof, and State law enforcement officers in subsection (a)(2) thereof to apply for pen register court orders, when the information sought is relevant to a legitimate criminal investigation.

-However, the definition of "legitimate criminal investigation" relates only to investigations or proceedings into a violation of "any Federal" criminal laws. No reference is made to State laws.

-Further, no authorization is granted for local law enforcement authorities to use pen registers. It is to be noted that Sec. 2516(2) of 18 USC permits local authorities to obtain electronic surveillance court orders under stated circumstances.

## 15. Sec. 3123: Contents of Order

It is suggested that Sec. 3123(b)(1)(C) be revised as follows:

> (C) the number and physical location of the telephone line to which the pen register is to be attached ...

Commentary:

The telephone number alone may not suffice to determine the correct telephone line. At times, law enforcement officials may have the incorrect telephone number. By requiring the physical location or address too, a further check is provided to ensure that the proper telephone line is authorized. Provision of such information also reflects general law enforcement practice today.

## 16. Sec. 3123: Nondisclosure of Existence of Device

Section 3123(d) prevents disclosure of an order authorizing use of a pen register for 60 days or the existence of the device; and this nondisclosure direction may be renewed for 60 day periods. However, it is the general practice of communications common carriers of the Bell System, which practice is still carried out after divestiture, not to notify customers in such situations.

Section 2511(2)(a)(ii) of 18 U.S.C ( as amended by Title II of the Foreign Intelligence Surveillance Act of 1978 - P.L. 95-511 ) prohibits any disclosure of the existence of any surveillance or surveillance device, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or the appropriate State or local prosecutor.

It is suggested that this provision be substituted for the 60-day provision of Section 3123(d). It is a flat prohibition against disclosure, except pursuant to legal process. It is easier for the courts, providers of service, and law enforcement to administer and reflects existing practice.

BEST COPY

### 17, Sec. 3124: Emergency Use of Pen Registers

(a) A law enforcement officer specially designated by the Attorney General may install and use a pen register device under Sec. 3124.

It is to be noted without recommendation that the Deputy Attorney General and the Associate Attorney General may authorize emergency interceptions under Title III (Sec. 2518(7) of 18 U.S.C. as recently amended by P.L. 98-473, approved October 12, 1984).

(b) It is to be further noted without recommendation that under Sec.2518(7) the principal prosecuting attorney of a State or political subdivision thereof may under appropriate enabling legislation authorize emergency interceptions without prior court order, subject of course to subsequent court approval. Sec. 3124 appears to be confined to Federal officials.

### 18. Sec. 3125:Assistance in Installation and Use of a Pen Register

(a) To be consistent with Sec. 2511(2)(a)(ii) of 18 U.S.C., as amended by Sec. 201 of Title II of Foreign Intelligence Surveillance Act, P.L.95-511 (October 1978), Sec. 3123(a)(1), which appear on Page 21 at Lines 5-6, should be revised to read as follows:

> (1) such assistance is directed by a court order signed by the authorizing judge as provided in section 3123(b)(2) of this title.

(b) To be consistent with Section 2511(2)(a)(ii) of 18 U.S.C., as amended by Sec. 201 of FISA ( P.L. 95-511 ),it is suggested that a new subsection (d) be added to Sec. 3125, to read as follows:

> (d) No cause of action shall lie in any court against any communication common carrier, landlord, custodian, or other person for providing information,facilities, or assistance in accordance with the terms of an order as provided in section 3123(b)(2) or as provided in section 3124 of this title.

(c) To be consistent with Section 2511(2)(a)(ii) as amended by FISA, it is suggested that Section 3125(a)(2) be revised to read as follows:

> (2) a certification in writing is provided by the law enforcement officer authorized to make the emergency installation and use of the pen register or tracking device as provided in section 3124 of this title, stating that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required. ( ~~the-emergency-installation-and-use-of-the-pen-register-or-tracking-device-is-authorized-under-section-3124 of-this-title-~~).

19. It is noted without recommendation that no order for physical entry is required for use of a pen register device or its installation. The U.S. Supreme Court has held that no separate order is required for physical entry when the electronic surveillance has be authorized by proper court order.

### 20. Sec. 3126(b)(2): Notice of Inventory Dispensed With

Section 3126(b)(1), which appears on Page 22 at Lines 16-17, provides that the serving of the pen register inventory may be postponed.

Section 3126(b)(2) provides for dispensing with service of the inventory when it would compromise an ongoing criminal investigation or result in the disclosure of classified information harmful to the national security. Clearly, notice should be dispensed with in the latter,national security situation.

- However, since service may be postponed, there seems to be no valid reason to dispense with notice entirely in ongoing criminal investigations. Notice can be postponed for a lengthy or indefinite period ( terminable when the investigation reaches a stage that it would no longer be compromised ).

- Under chapter 119, there is provision for suspension but not elimination of service of the inventory (Sec. 2518(8) ).

21. Should chapter 206 contain a provision similar to Section 2518(8)(a) pertaining to recordation, sealing, custody and retention ( for a 10 year period ) of pen register and, if appropriate, tracking device monitoring activities?

22. It is recommended that consideration be given to including in Section 3128 provisions similar to the suggestions contained on Page 4 of this Memorandum, namely,

- In Paragraph 8, entitled Sec. 103: Recovery of Civil Damages, and

- In Paragraph 9, entitled Sec. 103: Good Faith Reliance.

### 23. Sec. 3129: Court of Competent Jurisdiction

It is to be noted that in some instances State courts may be authorized by specifically enacted Court Rules, rather than a State statute, to issue a pen register or tracking device order. Such rules may be promulgated in furtherance of the court's inherent authority,or its statutory authority in areas where implementation of such authority is required.

- Accordingly, Congress may wish to give consideration to eliminating the phrase "authorized by a statute of that State" on Page 27 at Line 15 and substituting therefor the following:

(B) a court of general criminal jurisdiction of a State authorized ( ~~by a statute of that State~~ ) to enter orders authorizing the use of pen registers and tracking devices in accordance with this chapter.

○

H.W.W.C.